# FEDERACIÓN DE IDENTIDAD APLICADA A ENTORNOS EDUCATIVOS, UN ENFOQUE DE TECNOLOGÍAS SCIENCE GATEWAY: CASO DE ESTUDIO UNIVERSIDAD TECNOLÓGICA DE PEREIRA.

JHONNIER GUZMÁN GRANADA

UNIVERSIDAD TECNOLOGICA DE PEREIRA
FACULTAD DE INGENIERÍAS
MAESTRIA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA, 2020

# FEDERACIÓN DE IDENTIDAD APLICADA A ENTORNOS EDUCATIVOS, UN ENFOQUE DE TECNOLOGÍAS SCIENCE GATEWAY: CASO DE ESTUDIO UNIVERSIDAD TECNOLÓGICA DE PEREIRA.


Tesista:
**JHONNIER GUZMÁN GRANADA**

Director:
**LUIS EDUARDO SEPÚLVEDA RODRÍGUEZ**
Ing. MSc en Software Libre
Universidad Autónoma de Bucaramanga (UNAB).

Documento presentado como requisito para optar al título de:
**Magister en Ingeniería de Sistemas y Computación**

UNIVERSIDAD TECNOLOGICA DE PEREIRA
FACULTAD DE INGENIERÍAS
MAESTRIA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA, 2020

# Nota de aceptación

_____

_____

_____

_____
Jurado

_____
Jurado

Pereira, _____ de 2020.

# DEDICATORIA

*Dedico este proyecto de investigación a mi familia quienes han sido pilar fundamental para lograr mis metas, en especial a mi esposa por su invaluable apoyo, a mi madre por haber hecho de mi la persona que soy y a mi hija quien ha colmado mi vida de amor y felicidad.*

# AGRADECIMIENTOS

Mis mas sinceros agradecimientos a:

- Mi familia por estar siempre a mi lado.
- Mi director, MSc Luis Eduardo Sepúlveda Rodríguez, por su dedicación, paciencia, apoyo y orientación en el desarrollo de este proyecto.
- El equipo técnico de RENATA en cabeza de Carlos Ramirez, quienes dedicaron tiempo, conocimiento y buena voluntad a la integración de la UTP a la federación COLFIRE y a eduGAIN.
- El director de la Maestría en Ingeniería de Sistemas y Computación, por alentarme a finalizar la maestría y por sus buenas gestiones.
- La vicerrectoría de investigaciónes, innovación y extensión por compartir las capacidades identificadas en los grupos de investigación.
- A los docentes PhD Julio César Chavarro y Christian Candela por sus orientaciones y apoyo en la finalización del proyecto.
- Mis compañeros de la Administración de Redes y Seguridad de la información, por su colaboración y comprensión.

## Tabla de Contenidos

## Lista de tablas

## Lista de figuras

# 1 INTRODUCCIÓN

Aunque la gestión de identidad es un concepto simple en la teoría, se necesita que múltiples factores se cohesionen para lograr que dicho concepto funcione bien en la práctica. Es necesario planificar, diseñar y desarrollar cómo se va a implementar dicha gestión de identidad buscando el balance entre las expectativas del negocio, seguridad y experiencia de usuario. No existe una única propuesta ni una solución maestra que se ajuste a cada caso. (Wilson & Hingnikar, 2019).

La autenticación es la puerta de entrada a las aplicaciones. Debe ser una solución con alta disponibilidad y escalable, de lo contrario, podría convertirse en un obstáculo en lugar de una experiencia fácil y agradable a los usuarios.

El uso de múltiples usuarios y contraseñas para acceder a servicios y aplicaciones, ha sido y sigue siendo uno de los retos a los que se enfrentan las áreas de tecnologías de la información y que afectan la seguridad y la usabilidad de los recursos tecnológicos.

La autenticación centralizada, es una de las primeras aproximaciones que permite que diversas aplicaciones utilicen un repositorio central de usuarios, logrando que con las mismas credenciales, los usuarios puedan acceder a diferentes servicios. Esto es un gran avance y tiene beneficios desde el punto de vista del usuario final, así como para los administradores de TI, eliminando diferentes tecnologías que contienen usuarios lo que facilita la gestión de estos.

El protocolo ligero de acceso a directorios (LDAP) (Sermersheim, 2006) permite la autenticación de servicios y aplicaciones con un repositorio central de usuarios. Este protocolo es de amplia aceptación y tiene múltiples implementaciones tanto libres como Openldap y de pago como Directorio Activo de Microsoft entre otras.

El siguiente paso es la autenticación única para acceder a varias aplicaciones, conocido como inicio de sesión único o *Single Sign On* (SSO)(Shaer, 1995). Esta solución permite a los usuarios identificarse una sola vez y mantener la sesión válida para otras aplicaciones que hagan uso del SSO.

Protocolos como CAS, SAML y OpenID (Pérez Méndez, Marín López, & López Millán, 2016), son los más utilizados en las implementaciones de inicio único de sesión.

En entornos académicos en el año 2002 Klass Wierenga un exempleado de Cisco Systems, inició con un proyecto llamado EDUROAM (Education Roaming)(Wierenga & Florio, 2005) que pretendía dar acceso a las redes inalámbricas de las Universidades en el mundo, haciendo uso de las credenciales que cada miembro tenía de su institución. Dicha iniciativa tiene hoy en día 101 países alrededor del mundo.

El caso anterior es un ejemplo de una red federada, lo que en pocas palabras es tener muchas bases de datos en este caso de usuarios, las cuales funcionan como una sola entidad.

Luego surgió una nueva iniciativa de GEANT2 llamada EDUGAIN (Daryanani & Lopez, 2008), la cual busca brindar acceso de servicios y recursos tecnológicos a través de interferedación, lo cual es la interconexión de las redes federadas académicas y de investigación de cada país.

A través de la integración/implementación de la federación de identidad en entornos educativos y particularmente en la UTP, es posible conseguir las condiciones adecuadas para que se propicien diversos aspectos positivos como los que se detallan a continuación:

- Validación de identidad en diversos entornos evitando tener que recordar múltiples usuarios y contraseñas.
- Ingreso de credenciales una única vez para acceder a varios recursos tecnológicos.
- Ampliación del acceso a recursos tecnológicos disponibles en organizaciones que hacen parte de las redes académicas y que implementan federación de identidad.
- Oportunidades de cooperación interinstitucional que implementan federación de identidad.

# 2 DESCRIPCIÓN DEL PROBLEMA

La masiva aceptación de las tecnologías de la información en los entornos educativos, entre otros aspectos, hace que hoy en día sea común el uso de recursos tecnológicos que entregan valor en diversos ámbitos, sin embargo, estos recursos por lo general traen consigo sistemas o módulos de gestión de usuarios para validar su acceso, lo que conlleva a enfrentar al usuario a situaciones problémicas como las siguientes:

- Necesidad de validar su identidad en diversos entornos teniendo que recordar en algunas ocasiones diferentes usuarios y contraseñas.
- Por lo general debe ingresar sus credenciales en cada recurso que requiera usar.
- Limitado acceso a recursos tecnológicos disponibles en organizaciones que hacen parte de las redes académicas y que implementan federación de identidad.
- Limitación de la UTP para aprovechar oportunidades de cooperación interinstitucional que implementan federación de identidad

# 3 OBJETIVOS

## 3.1 OBJETIVO GENERAL

Aplicar federación de Identidad a entornos educativos buscando un enfoque science gateway: caso de Estudio Universidad Tecnológica de Pereira.

## 3.2 OBJETIVOS ESPECÍFICOS

1. Identificar problemas, necesidades y oportunidades de la Universidad Tecnológica de Pereira, con relación a la federación de identidad.

2. Seleccionar tecnologías existentes para federación de identidad que satisfagan los problemas, necesidades u oportunidades del objetivo anterior.

3. Construir un esquema arquitectónico para la implementación de federación de identidad en la UTP.

4. Implementar un prototipo funcional de federación de identidad para el esquema arquitectónico definido.

# 4 MARCO TEÓRICO

## 4.1 AUTENTICACIÓN VS. AUTORIZACIÓN

Son dos términos relacionados con seguridad que las personas tienden a confundir. Autenticación es verificar la identidad mientras Autorización es verificar que se tiene acceso a un recurso. (Ver **Ilustración 1**)

Autenticación es validar las credenciales en un login antes de dar accesos a un sistema. Desde el punto de vista de seguridad, se recomiendan al menos dos factores de autenticación antes de otorgar accesos.

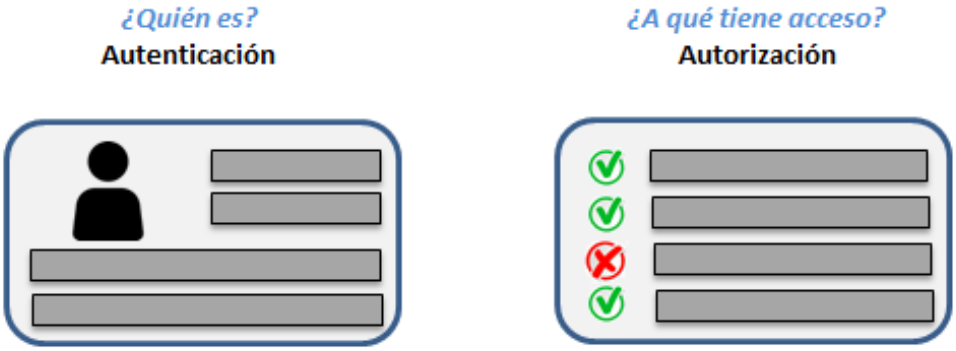



***Ilustración 1*** *Autenticación vs. Autorización*[1]

La Autorización ocurre después de un proceso de Autenticación verificando los permisos antes de otorgar los accesos solicitados por recursos como bases de datos,

[1] Fuente: Del autor

archivos, repositorios, etc. Tanto la Autenticación como la Autorización son cruciales para la gestión de la Seguridad.

## 4.2 IDENTIDAD

Se define como Identidad el conjunto de atributos asociados a una persona o entidad específica en un contexto particular (Wilson & Hingnikar, 2019). Una identidad puede incluir uno o más atributos. Para el caso de identidades humanas, se pueden citar ejemplos como el nombre, la edad, la dirección de residencia, número telefónico, color de ojos. Para el caso de identidades no-humanas, se pueden dar como ejemplos un propietario, identificador, dirección IP, modelo, versión. Estos atributos pueden ser usados en los procesos de autenticación y autorización.

Un sistema de gestión de identidad (IdM Identity Management System) es un conjunto de servicios que soportan la creación, modificación y eliminación de identidades; así como también involucra la autenticación y la autorización. Estos sistemas son usados para evitar los accesos no autorizados a los recursos y constituyen una parte importante de un modelo de seguridad.

## 4.3 EVOLUCIÓN DE IDENTIDAD

A continuación se hará un recorrido por los enfoques que se han usado en el pasado para gestionar los datos de identidad, autenticación y autorización, basados en (Wilson & Hingnikar, 2019). Varios de ellos todavía se usan. Conocer las ventajas y desventajas de cada uno de ellos, permitirá evaluar de forma efectiva las alternativas.

### 4.3.1 Identidad por aplicación

Es el primer tipo de autenticación que se llegó a usar. Hace varios años, cada aplicación tenía su propia base de datos u otro tipo de almacenamiento para guardar la identidad y perfil de sus usuarios y funcionaban de forma aislada. Cada aplicación solicitaba las credenciales a los usuarios y las validaban contra su propio repositorio de información. Esto implicaba que cada usuario podría tener un usuario/contraseña diferente por cada aplicativo que tuviera que acceder, con todas las dificultades que esto pudiera conllevar, por ejemplo, si algún dato del perfil del usuario cambiaba, éste debía ser actualizado en múltiples aplicaciones; el usuario se veía obligado a memorizar numerosos usuarios/contraseñas o a utilizar las mismas credenciales en diferentes aplicativos, con el agravante de que si una de las aplicaciones se veía comprometida en asuntos de seguridad, se ponía en riesgo el resto de datos en las demás aplicaciones. Este enfoque, es aún utilizado por algunas compañías.

### 4.3.2 Repositorio centralizado de usuarios

Con el tiempo, cada vez se generaron más aplicativos para entornos empresariales. Esto conllevó a buscar un mejor enfoque para la gestión de los usuarios. Se implementaron

servicios de directorios para almacenar y centralizar la información de las identidades de los usuarios. Como ventajas de este enfoque se pueden citar las siguientes:

- Eliminación de inconsistencia de datos al tener la información del usuario centralizada.
- El mismo usuario/contraseña se puede usar en diferentes aplicaciones.
- Único punto de control para implementar políticas de contraseñas o bloquear usuarios, si es requerido.

Debido a lo anterior, los servicios de directorio fueron ampliamente adoptados, al menos, en las grandes empresas. Sin embargo, también se tenían algunas desventajas como el servicio de directorio por sí solo no gestiona una sesión de usuario; aunque el usuario sólo debe recordar un nombre/contraseña, de todas formas debe ingresar sus credenciales en cada aplicativo y finalmente, se tenía un único punto de fallo convirtiéndose en un riesgo.

Uno de los servicios de directorio más conocido es LDAP (Lightweight Directory Access Protocol). Fue desarrollado por la Universidad de Michigan y la IETF (Internet Engineering Task Force) como un conjunto de servicios de red que provee gestión de objetos y acceso a través de TCP/IP. LDAP es un protocolo orientado a mensajes. Cuando un cliente LDAP necesita un dato específico en un servidor LDAP, el cliente genera un mensaje que contiene la solicitud y lo envía al servidor LDAP. El servidor extrae el dato de su base de datos y los envía al cliente en un mensaje LDAP. Adicional, retorna un

código de resultado al cliente en un mensaje separado para finalizar la sesión. La **Ilustración 2** presenta la interacción entre un cliente y servidor LDAP.

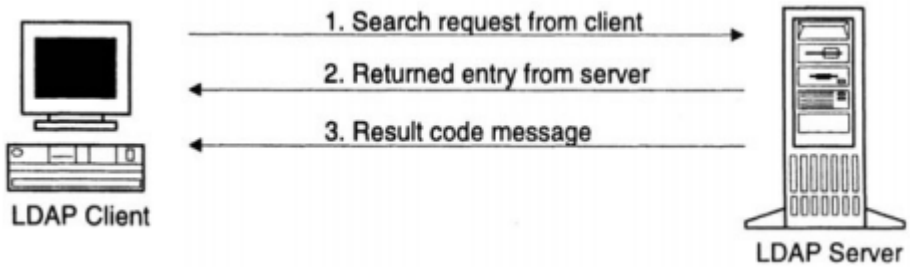



***Ilustración 2*** *Operación LDAP*[2]

### 4.3.3 Single Sign On

*Single Sign On* (SSO) introdujo algunas mejoras a lo expuesto anteriormente. Los servidores de SSO tomaban la información de identidad de un servicio de directorio, pero incluía una capa sobre este servicio para mantener la información de las sesiones de los usuarios que ya se habían autenticado. En un flujo típico, una aplicación redirecciona al usuario a un servidor SSO para gestionar la autenticación del usuario y recibir sus datos de una forma segura. Si el usuario accedía a una segunda aplicación, ésta redirigía al usuario al servidor SSO quien podía detectar si ya existía una sesión váida del usuario y de esta forma, regresarlo al aplicativo con una respuesta exitosa para la autenticación sin que el usuario deba digitar nuevamente sus credenciales. Se pueden citar los siguientes beneficios de este esquema sobre el visto en el punto anterior:

---

[2] Fuente: *("Database Appl. Secur. XV," 2002)*

- Facilidad para el usuario al poder acceder a diferentes aplicaciones con una única autenticación.
- Los equipos encargados de seguridad lo prefieren ya que las credenciales del usuario sólo son expuestas al servidor SSO en lugar de cada aplicación.
- Único punto para definir políticas de autenticación.

Sin embargo, también tiene desventajas como que su implementación puede ser costosa en tiempo, por lo que su adopción es más frecuente en grandes empresas que tienen los recursos para integrar sus aplicaciones a los servidores SSO. Adicional, SSO se basa en cookies que los navegadores frecuentemente bloquean, lo que hace que esta solución funcione dentro de un mismo dominio de internet. Dado que muchas compañías están optando por aplicaciones externas como *Software As A Service* (SaaS[3]), esta es una restricción bastante importante.

### 4.3.4 Federación de Identidad

Hoy en día la gestión de identidades involucra a compañías e instituciones académicas. Entre los diferentes modelos que existen, el modelo de federación es el único que asegura protección en términos de privacidad. (De Angelis, Falcioni, Ippoliti, Marcantoni, & Re, 2013)

---

[3] SaaS: *Software As A Service*, modelo de distribución de software en el cual una tercero provee servicios de alojamiento de aplicaciones y las pone a disposición de los usuarios a través de internet. (Familiar, 2015)

La creciente demanda de aplicaciones bajo SaaS creó nuevos desafíos para la gestión de identidad. Las compañías empezaron a tener dificultades para gestionar las identidades de sus usuarios en aplicaciones SaaS y de nuevo, los usuarios debieron recordar una contraseña por cada aplicación. Afortunadamente, ya existen estándares que proveen una solución para SSO web sobre diferentes dominios y federación de identidad. De esta forma, las aplicaciones SaaS redireccionan a los usuarios a un servicio corporativo de autenticación conocido como Proveedor de Identidad (IdP). La federación de identidad, de esta manera, proporcionó una forma de vincular una identidad utilizada en una aplicación con un dentidad en el IdP y permitió que las empresas tengan las ventajas de un SSO tanto con aplicaciones internas como con SaaS.

## 4.4 SSO

*Single Sign On* (SSO) es un mecanismo que permite que un usuario se autentique en un sistema una única vez accediendo a todos los recursos que tenga autorizados sin necesidad de digitar nuevamente sus credenciales en cada aplicación a la que desee ingresar. (Chun & Katuk, 2014).

Tal como lo menciona (Wilson & Hingnikar, 2019), Single Sign On es posible sólo si un conjunto de aplicaciones ha delegado la autenticación a una única entidad. Una sesión en esta entidad puede ser usada para otorgar acceso a múltiples recursos vía *Single Sign On*.

*Single Sign On* puede facilitar la autenticación en varios escenarios. En entornos comerciales, un usuario puede disfrutar de varias aplicaciones permitiendo autenticarse vía Google. En un entorno empresarial, un empleado puede ingresar a diferentes aplicativos aprovechando el proveedor de identidad de su compañía. En un entorno educativo, los estudiantes, profesores y administrativos pueden disfrutar de múltiples servicios o aplicaciones haciendo uso de un proveedor de identidad académico.

**Beneficios de SSO:**

Para usuarios finales:

- Facilidad en la autenticación
- Menos usuarios y contraseñas a aprender y exponer

Para compañías que publican aplicaciones:

- Menos esfuerzo requerido para desarrollar módulos de autenticación
- Único sitio para implementar políticas de autenticación, recuperación de credenciales, eliminación de cuentas, implementación de seguridad.

**Riesgos**

- Su implementación puede generar un único punto de fallo.
- El servicio centralizado de autenticación puede ser un punto de interés para ataques.

### 4.4.1 Cómo funciona SSO

Usando el ejemplo presentado en la **Ilustración 3** el usuario visita la aplicación 1 la cual redirecciona el navegador a un Proveedor de Identidad con una solicitud de autenticación. El Proveedor de Identidad autentica el usuario, establece una sesión y crea una cookie en el navegador con la información de la sesión. Luego, se redirecciona nuevamente a la aplicación con el token de seguridad, el cual contiene datos acerca de la autenticación y del usuario. La aplicación puede crear o actualizar su sesión local. Si el usuario visita la aplicación 2 con el mismo navegador, la segunda aplicación detecta que el usuario ya está autenticado y entonces redireccoina al Proveedor de Identidad. El navegador incluye la cookie con la solicitud, así el Proveedor de Identidad usa esta cookie para detectar que el usuario ya tiene una sesión autenticada. Verifica que dicha sesión todavía sea válida y si es así, redireccionade nuevo a la segunda aplicación con el token sin solicitarle al usuario las credenciales. La aplicación 2 crea o actualiza su sesión local. De esta forma, el usuario puede continuar con el acceso a aplicaciones subsequentes sin necesidad de entregar nuevamente sus credenciales.

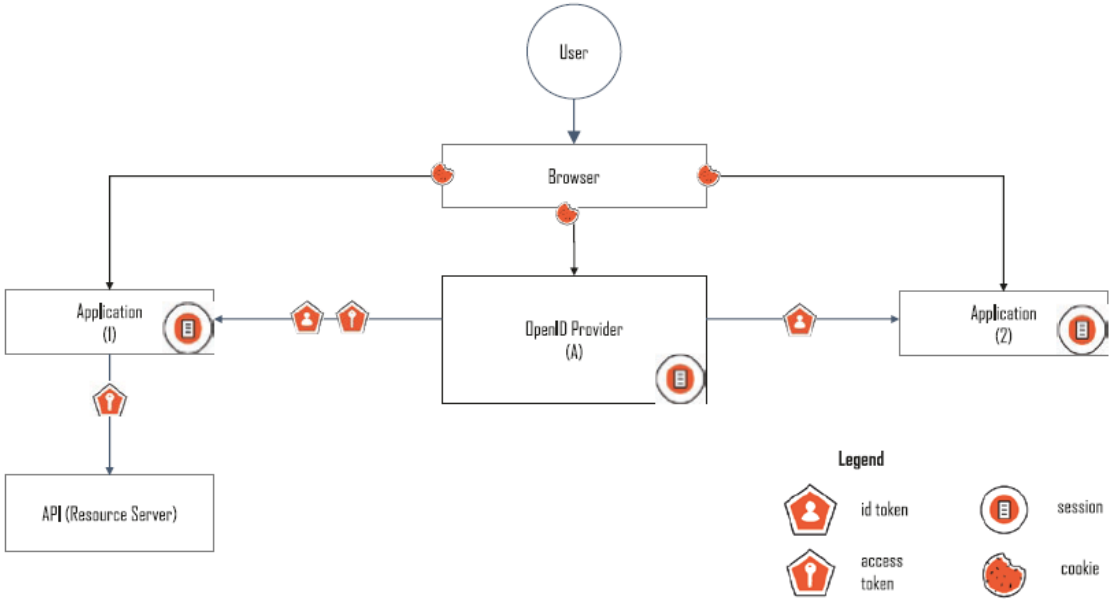



***Ilustración 3*** *Funcionamiento SSO*[4] .

## 4.5 SLO

Logout puede ser algo sobre lo que no se suele pensar con frecuencia, pero puede ser incluso más complejo de diseñar y probar que un login. Para las aplicaciones, es importante que los usuarios cuenten con una forma de finalizar su sesión. *Single LogOut* (SLO) se encarga de finalizar las sesiones de una forma controlada en entornos SSO.

### 4.5.1 Múltiples sesiones

[4] Fuente: *(Wilson & Hingnikar, 2019)*

Tal como lo indica (Wilson & Hingnikar, 2019), el *logout* puede ser complejo en entornos con SSO debido a la cantidad de sesiones activas que se deben finalizar. La **Ilustración 4** presenta diferentes escenarios para sesiones de autenticación. En el modelo 1, se presenta una sesión de aplicación. Si la aplicación delega la autenticación a un Proveedor de Identidad (IdP), éste también tendrá una sesión de usuario (Modelo 2). Si la aplicación además, usa un servidor de descubrimiento (*authentication broker*) para facilitar el uso de diferentes proveedores de identidad, el servidor de descubrimiento también tendrá una sesión de usuario activa (Modelo 3). Esto significa que el usuario puede tener sesiones activas en tres capas en la arquitectura o incluso más, si el proveedor de identidad delega la autencación a otro IdP.

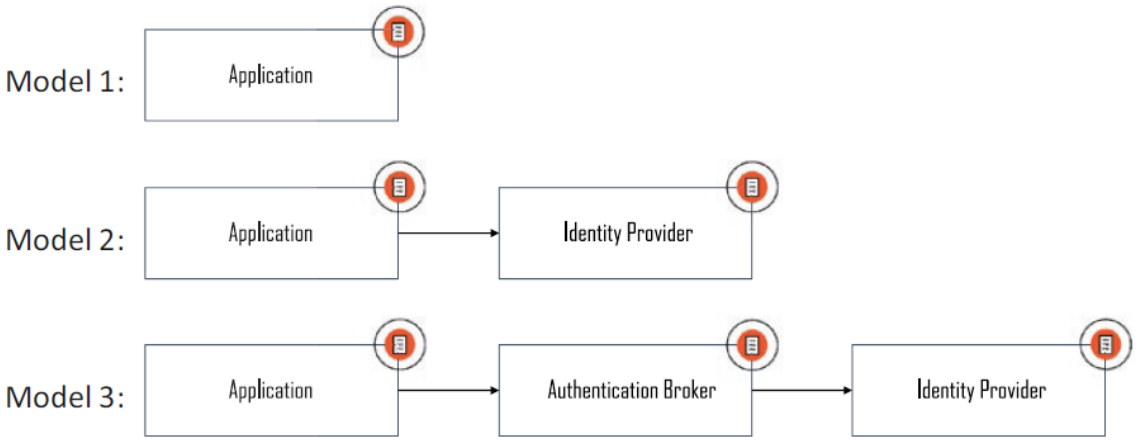



***Ilustración 4*** *Múltiples sesiones de Usuario*[5]

[5] Fuente: *(Wilson & Hingnikar, 2019)*

### 4.5.2 Opciones de *Logout*

Cuando se tienen los escenarios de los modelos 2 y 3 (**Ilustración 4**), es necesario decidir qué debe suceder si alguna de las sesiones de usuario se finaliza. Si una sesión de usuario se termina en una aplicación, puede ser apropiado finalizar una o más de las sesiones subsiguientes, si existen:

- Sesión de aplicación
- Sesión en servidor de descubrimiento
- Sesión en proveedor de identidad

Así mismo, si la sesión que se finaliza es en el proveedor de identidad o en el servidor de descubrimiento, puede ser necesario terminar una o más de las sesiones de usuario en alguna de las capas involucradas (aplicaciones u otros proveedores).

Para definir el *logout*, es necesario considerar dónde existen las sesiones y cuáles deberían ser finalizadas cuando el usuario inicia un logout o si su sesión se termina por otras razones. Uno de los factores de decisión depende del propietario de las sesiones. En entornos empresariales, las políticas de seguridad pueden indicar que el *logout* en una aplicación debe disparar la finalización de las sesiones en los proveedores de identidad y posiblemente en toda aplicación donde el usuario tenga sesiones activas. Una vez que el *logout* ha sido implementado, es necesario destinar el tiempo suficiente a realizar pruebas exhaustivas que validen el funcionamiento de acuerdo con el diseño planteado.

## 4.6 EVENTOS EN LA VIDA DE UNA IDENTIDAD

Después de conocer los términos anteriores, es válido presentar los principales eventos que ocurren durante la vida de una identidad, presentada en la **Ilustración 5**.

### 4.6.1 Aprovisionamiento

Es el primer paso en la vida de una identidad. Se refiere a la creación de una cuenta y su asociación con la información de la identidad. Se puede realizar registrando un usuario, importando información de identidad de un sistema heredado o delegando a un servicio de identidad externo. El objetivo de esta fase es establecer una relación directa entre una cuenta y los datos de identidad asociados obteniendo o asignando un identificador único. Ejemplo: registro en servicios bancarios. El banco presenta un formulario de registro que diligencia el usuario con unos datos básicos. Estos datos son usados para aprovisionar una cuenta en línea en el banco asociada al usuario que hizo la solicitud.

### 4.6.2 Autorización

Después de la creación de la cuenta, es necesario especificar qué puede realizar (otorgar privilegios).

### 4.6.3 Autenticación

El usuario debe autenticarse para validar el acceso. El usuario entrega un identificador para obtener la cuenta e ingresar las credenciales. Éstas son validadas contra las credenciales previamente registradas durante la fase de aprovisionamiento.

### 4.6.4 Aplicación de políticas de acceso

Una vez que el usuario ha sido autenticado y asociado con una cuenta, es necesario aplicar las políticas de acceso para asegurar que las acciones del usuario están permitidas por los privilegios que le han sido otorgados.

### 4.6.5 Sesiones

Después de la autenticación y la autorización, se ejecutan varias acciones en la aplicación como gestionar la sesión validando que el usuario permanezca activo por un período de tiempo limitado.

### 4.6.6 Single Sign On (SSO)

Después de que el usuario accede una aplicación, puede desear realizar alguna actividad que involucre otra aplicación. En este caso, puede hacer uso de SSO para habilitar el acceso sin necesidad de digitar nuevamente sus credenciales.

### 4.6.7 Autenticación fuerte

Se puede involucrar la autenticación por múltiples factores. Adicional al usuario y contraseña, se usan otras formas de autenticación conocidas como fuertes, las cuales pueden incluir: algo que el usuario tenga, algo que el usuario conozca y/o biometría.

### 4.6.8 Logout

Se trata de finalizar la sesión cuando el usuario lo indique o por otros factores como tiempo límite o tiempo de inactividad. En casos de SSO, se deben tener en cuenta múltiples sesiones para finalizar, tal como se ha presentado en el apartado de SLO.

### 4.6.9 Gestión de la cuenta y recuperación

Se trata de actualización de atributos de la cuenta si así se requiere y la recuperación de credenciales si se ha olvidado el usuario o la contraseña.

### 4.6.10 Desaprovisionamiento

Es el cierre de una cuenta, si así es requerido. En este caso, la cuenta del usuario y la información de identidad deben ser marcadas como inactivas para que el usuario no pueda volver a usarlos para autenticarse.


***Ilustración 5*** *Eventos en la vida de una identidad*[6]

## 4.7 SCIENCE GATEWAY

*Science gateways*, laboratorios y entornos virtuales de investigación se refieren a varios tipos de interfaces digitales desarrolladas para avanzar en las tecnologías avanzadas

[6] Fuente: *(Wilson & Hingnikar, 2019)*

que apoyan la investigación. Se utilizan en una amplia variedad de dominios científicos, desde física de alta energía y astrofísica hasta en humanidades y las ciencias sociales.

Al adaptar entornos digitales a las necesidades de la comunidad, *science gateways* desempeñan un papel clave en la integración de elementos en el ámbito de la infraestructura electrónica, proveyendo acceso en línea a software, datos, colaboración herramientas, instrumentación y computación de alto desempeño, para facilitar mayores impactos de la investigación. (Barker et al., 2019)

## 4.8 INFRAESTRUCURA DE AUTENTICACIÓN Y AUTORIZACIÓN

Muchas organizaciones usan Infraestructuras de Autenticación y Autorización (AAI) para construir un entorno confiable donde los usuarios puedan ser identificados electrónicamente usando una sola identidad. La necesidad de que la identidad del usuario cruce las fronteras entre organizaciones, dominios y servicios, lleva a la creación de entornos de identidad federados.

Una federación de identidad es un grupo de proveedores de identidad y servicios que se suscriben a un conjunto acordado de políticas para intercambiar información sobre usuarios y recursos para permitir el acceso y uso de los recursos. Hay muchas federaciones de identidad de Investigación y Educación en todo el mundo y comúnmente tienen una cobertura nacional.

## 4.9 FEDERACION DE COLOMBIA – COLFIRE

La Federación Colombiana de Identidad para la Investigación y la Educación (ColFIRE) es una federación de identidad que reúne instituciones de enseñanza e investigación en Colombia. A través de ColFIRE, un usuario guarda toda su información en la institución de origen y puede acceder a los servicios ofrecidos por las instituciones que participan en la federación ("Colfire - Red RENATA," 2020).

## 4.10 INTERFEDERACIÓN – eduGAIN

eduGAIN es un servicio de interfederación que interconecta federaciones de identidad en todo el mundo, simplificando el acceso a contenido, servicios y recursos para la comunidad global de investigación y educación. La tecnología eduGAIN implica un "servicio de metadatos", que regularmente recupera y agrega información de las federaciones participantes sobre proveedores de servicios e identidades, y pone esta información a disposición de las federaciones. eduGAIN coordina los elementos necesarios de la infraestructura técnica de las federaciones y proporciona un marco de políticas que controla el intercambio de esta información entre las Federaciones de Identidad.

La siguiente imagen (**Ilustración 6**) presenta las redes federadas por país que existen en eduGAIN a enero del 2020.

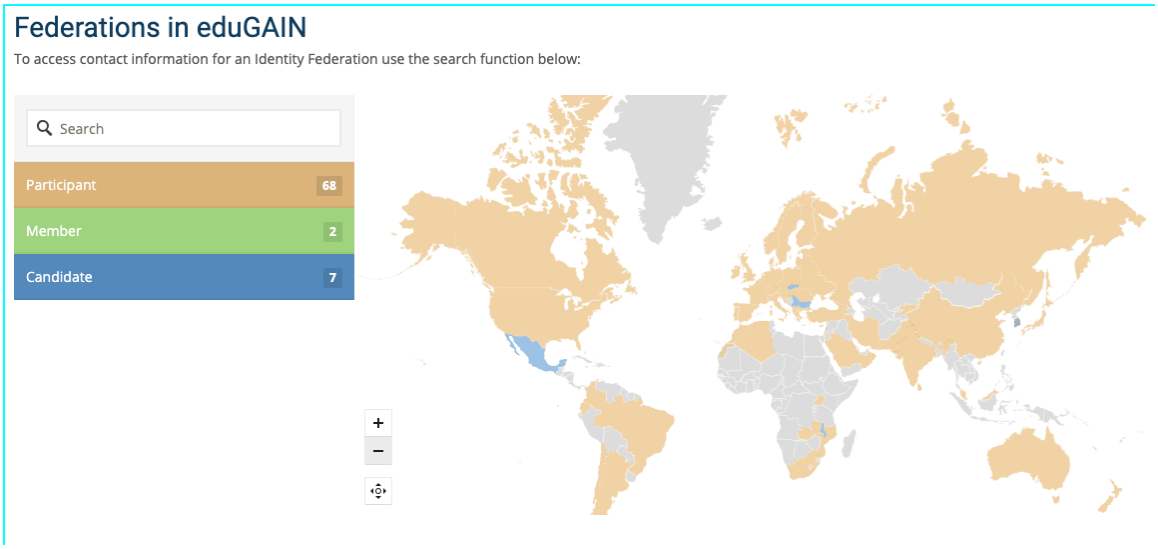



***Ilustración 6*** *Federaciones que hacen parte de eduGAIN*[7]

Cuenta con 68 países participantes (Federaciones por país), 2 miembros (Participan en las decisiones administrativas pero no cuentan con federación de identidad) y 7 candidatos (pendientes por aprobación para ser participante).

Para que una institución académica haga parte de eduGAIN, requiere hacer parte de la red académica nacional de su país.

eduGAIN proporciona una forma eficiente y flexible para que las federaciones participantes, sus usuarios y servicios afiliados se interconecten. Hoy en día los servicios en línea son cruciales para la investigación y la educación. Estudiantes, profesores,

[7] Fuente: ("eduGAIN – enabling worldwide access," 2020)

investigadores y personal de la institución, hacen uso de gran variedad de servicios web, tales como cursos en línea, análisis e intercambio de datos, acceso a revistas y bibliotecas, etc. Permitir un acceso fácil y conveniente a los usuarios es una parte clave de la prestación de un servicio. Los proveedores de servicios no desean los dolores de cabeza asociados con la emisión de contraseñas a los usuarios, y el usuario no quiere otra contraseña.

Con solo una identidad confiable proporcionada por la institución del usuario como parte de una federación de identidad que participa en eduGAIN, los usuarios pueden acceder a los servicios de otras federaciones participantes. También funciona con inicio de sesión único (SSO), por lo que el usuario necesita iniciar sesión solo una vez durante una sesión del navegador.

Las federaciones de identidad generalmente se implementan a nivel nacional y utilizan diferentes arquitecturas, sistemas y políticas. eduGAIN permite que las federaciones de identidad se interconecten, de modo que las instituciones y servicios participantes puedan colaborar sin la necesidad de establecer conexiones bilaterales individuales. Esta es la puesta en escena de interfederación.

# 5 FEDERACIÓN DE IDENTIDAD PARA LA UNIVERSIDAD TECNOLÓGICA DE PEREIRA

## 5.1 VALORACIÓN DEL GRUPO OBJETIVO

Como estrategia para realizar la valoración de los problemas, necesidades y oportunidades en la UTP, se realizó entrevista guíada a los tomadores de decisiones y se utilizaron datos de los grupos de investigación recolectados por la vicerrectoría e investigaciones y extensión.

### 5.1.1 Identificación de problemas y necesidades

La estrategia utilizada para identificar los problemas y necesidades que tiene la Universidad Tecnológica de Pereira con relación a los recursos y servicios computaciones institucionales fue realizar entrevista con el vicerrector administrativo y financiero, la jefe de Gestión de Tecnologías Informáticas y Sistemas de Información y el director del Centro de Recursos Informáticos y Educativos, la cual se realizó el día 21 de enero a las 10 am y en donde se identificó lo siguiente:

**Problemas**

- Ejecución presupuestal atomizada, distribuidos entre facultades, grupos de investigación e investigadores.
- Existencia de recursos costosos que no se comparten entre grupos de investigación.
- Recursos existentes con capacidades computacionales desaprovechadas.

**Necesidades**

- Aprovechar mejor los recursos existentes.
- Dar a conocer las capacidades de los grupos de investigación.
- Orientar  inversiones en adquisición tecnológica.

### 5.1.2 Identificación de oportunidades

Como estrategia para la identificación de oportunidades, se utilizó como base los documentos obtenidos por la Vicerrectoría de Investigaciones, Innovación y Extensión de la UTP, quienes desde el 2018 han iniciado la tarea de identificar las capacidades que tienen los grupos de investigación. Como fruto de este trabajo para el 2020 resultaron un conjunto de fichas técnicas de 76 grupos de investigación. Es de resaltar que las capacidades de los grupos de investigación encontradas en este estudio son consideradas como insumo para determinar las oportunidades con respecto a federación de identidad en la UTP.

A continuación se muestran resultados relevantes del estudio de la UTP que nos permita caracterizar el grupo objetivo en este trabajo.

Para enero de 2019 tal como se muestra en **Ilustración 7** existen un total de 125 grupos de investigación, de los cuales 114 están reconocidos por Colciencias y 11 grupos registrados en Colciencias (Vicerrectoría de investigaciones, 2020). De este total, se incluyen 76 grupos de investigación en el estudio, que corresponden a las fichas técnicas recibidas.

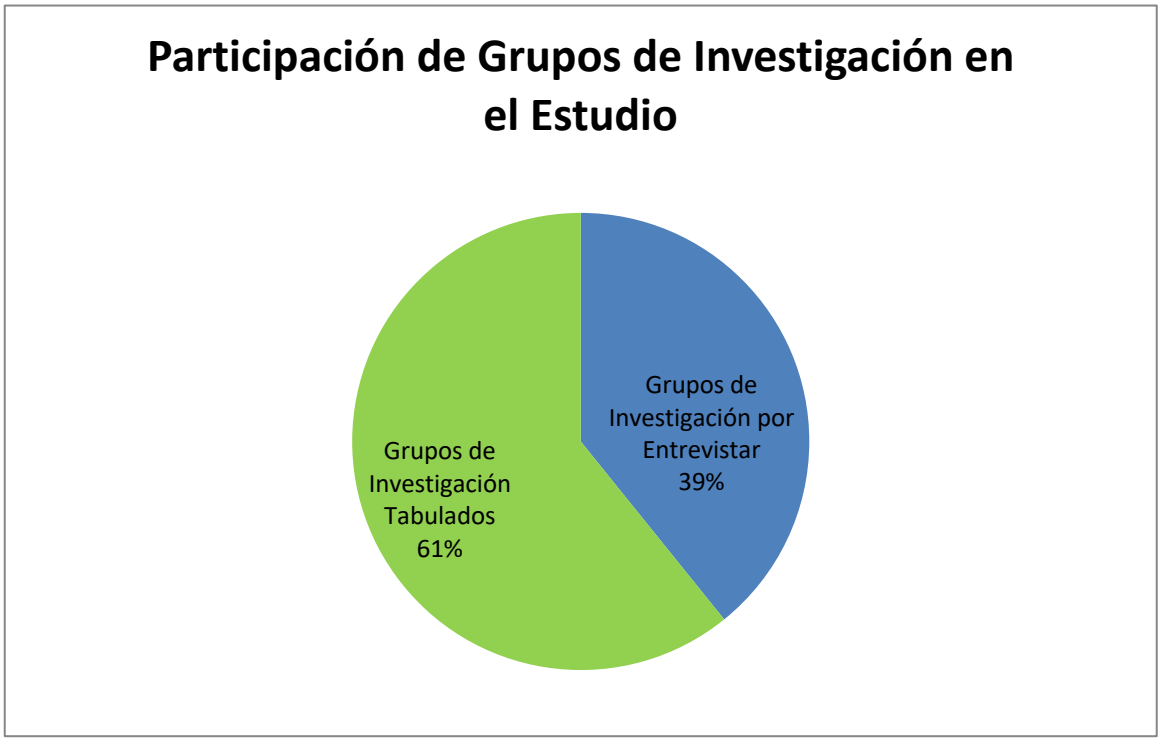



***Ilustración 7*** *Participación de Grupos de Investigación en Estudio*[8]

[8] **Fuente:** Del autor

### *5.1.2.1 Cantidad de Grupos de Investigación por Área de Interés*

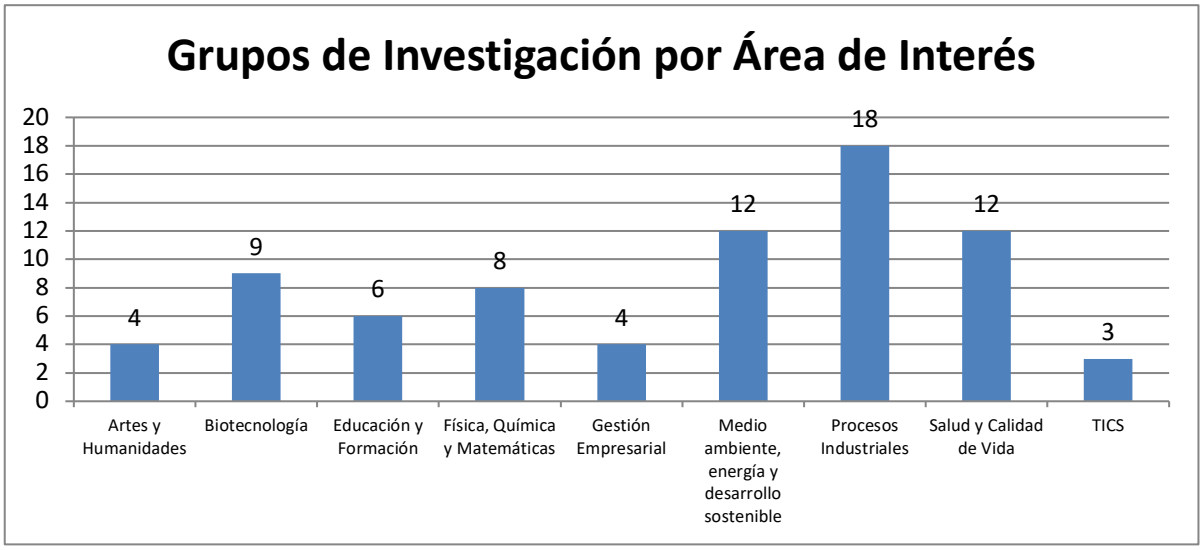



***Ilustración 8*** *Cantidad de Grupos de Investigación por Área de Interés*[9]

Las áreas de interés que presentan mayor número de grupos de investigación son "Procesos Industriales", "Medio Ambiente, Energía y Desarrollo Sostenible" y "Salud y Calidad de Vida". (Ver **Ilustración 8**)

### *5.1.2.2 Participación de los grupos de investigación por Categoría*

[9] **Fuente:** Del autor

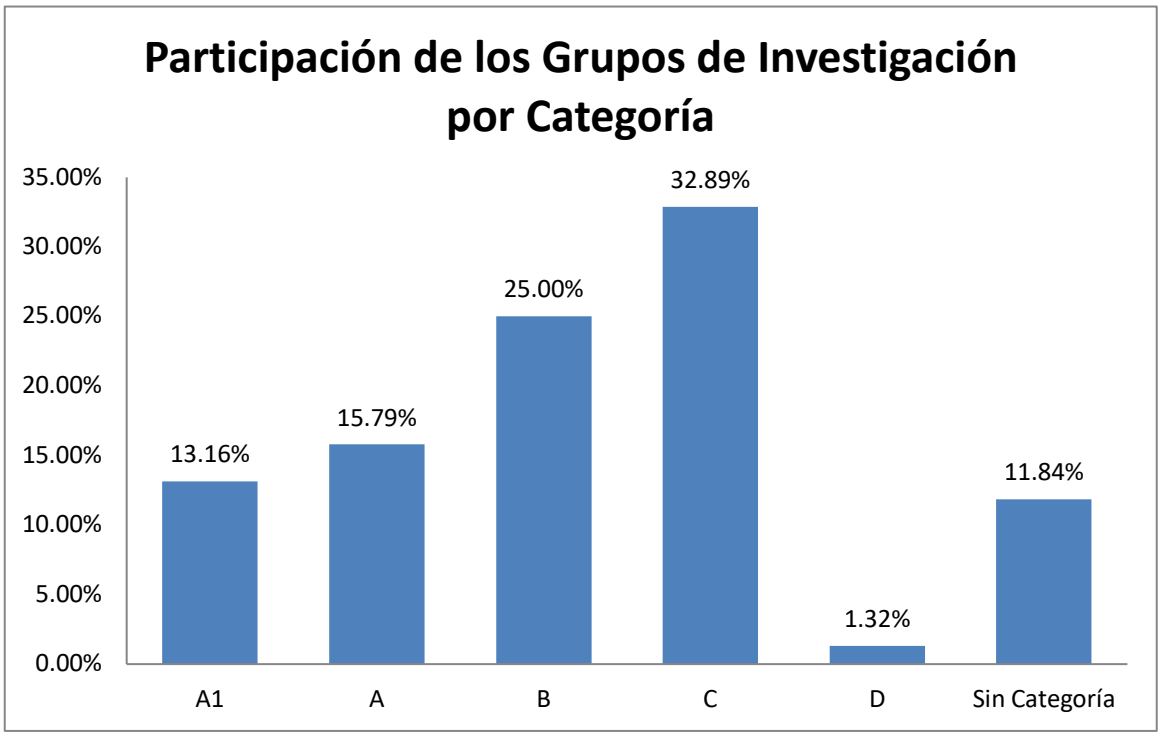



***Ilustración 9*** *Participación de los grupos de investigación por Categoría*[10]

Se encuentra que la mayor participación de los grupos de investigación se halla en la Categoría C. Del total de grupos tabulados, solo el 13,16% tienen la máxima categoría (Ver **Ilustración 9**).

[10] **Fuente:** Del autor

### *5.1.2.3 Categorías de los grupos de investigación por área de interés*

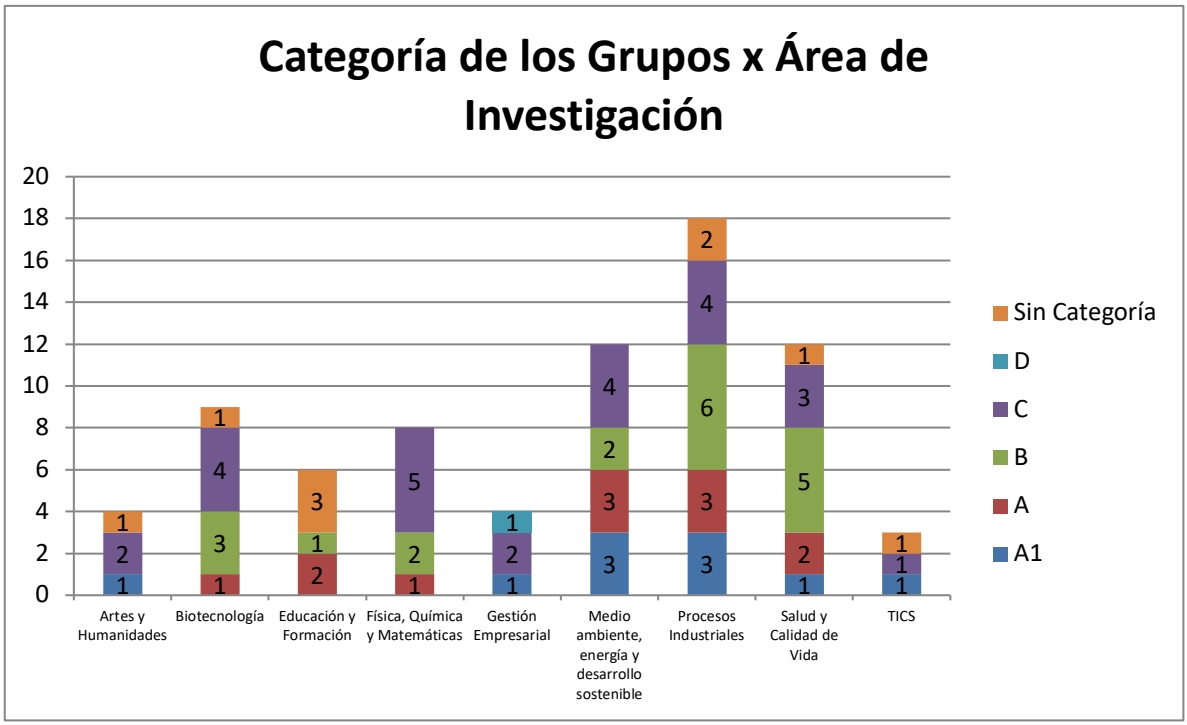



***Ilustración 10*** *Categorías de los grupos de investigación por área de interés*[11]

En la **Ilustración 10** se identifica que las áreas de interés "Física, Química y Matemáticas", "Gestión Empresarial" y "Medio Ambiente, Energía y Desarrollo Sostenible" tienen todos sus grupos de investigación categorizados. Los grupos de investigación A1 se encuentran concentrados en las áreas de interés que mayor cantidad de grupos tienen.

[11] **Fuente:** Del autor

### *5.1.2.4 Participación de Recursos por Área de Interés*

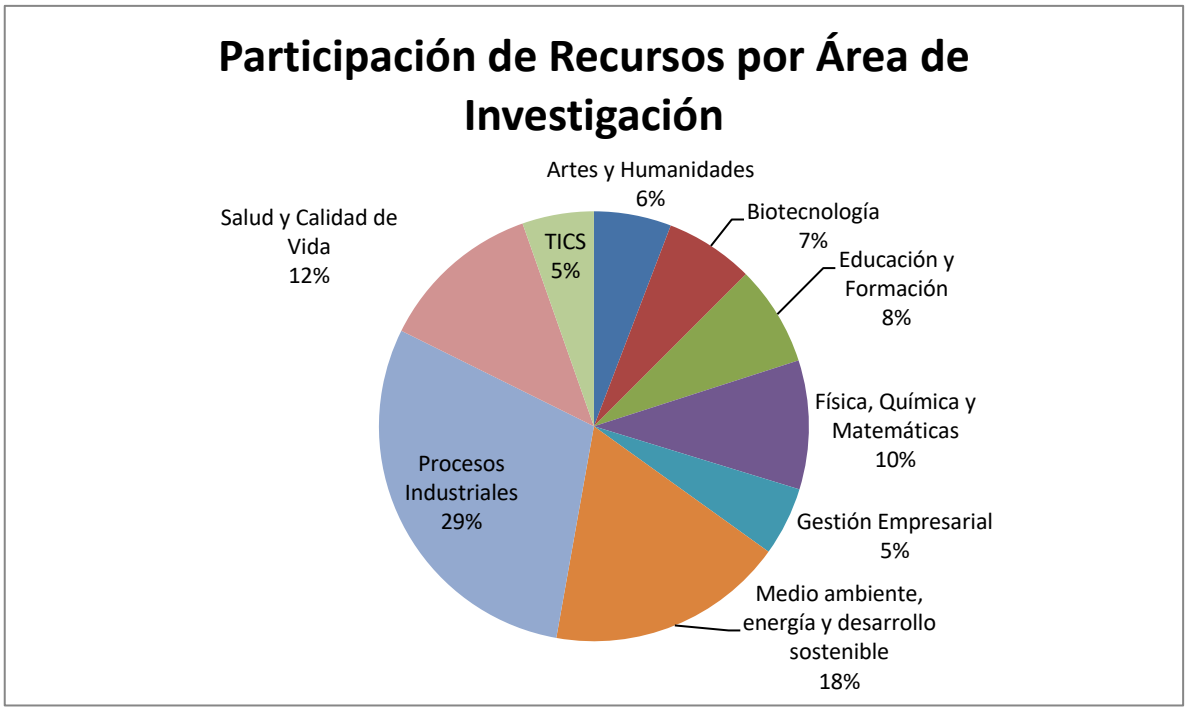



***Ilustración 11*** *Participación de Recursos por Área de Interés*[12]

Como era de esperarse, el área de interés que mayor número de recursos o capacidades ha producido, es "Procesos Industriales" ya que es la que tiene el mayor número de grupos de investigación (Ver **Ilustración 11**). El total de recursos identificados es 464.

[12] **Fuente:** Del autor

### *5.1.2.5 Recursos por Grupo de Investigación*


***Ilustración 12*** *Recursos por Grupo de Investigación*[13]

El ranking de grupos de investigación que más recursos o capacidades han generado, están adscritos a Ingeniería Eléctrica. (Ver **Ilustración 12**)

[13] **Fuente:** Del autor

### *5.1.2.6 Recursos candidatos a Federar por Área de interés*

Se han seleccionado como candidatos a ser federados los recursos identificados como computacionales, software, equipos y prototipos.

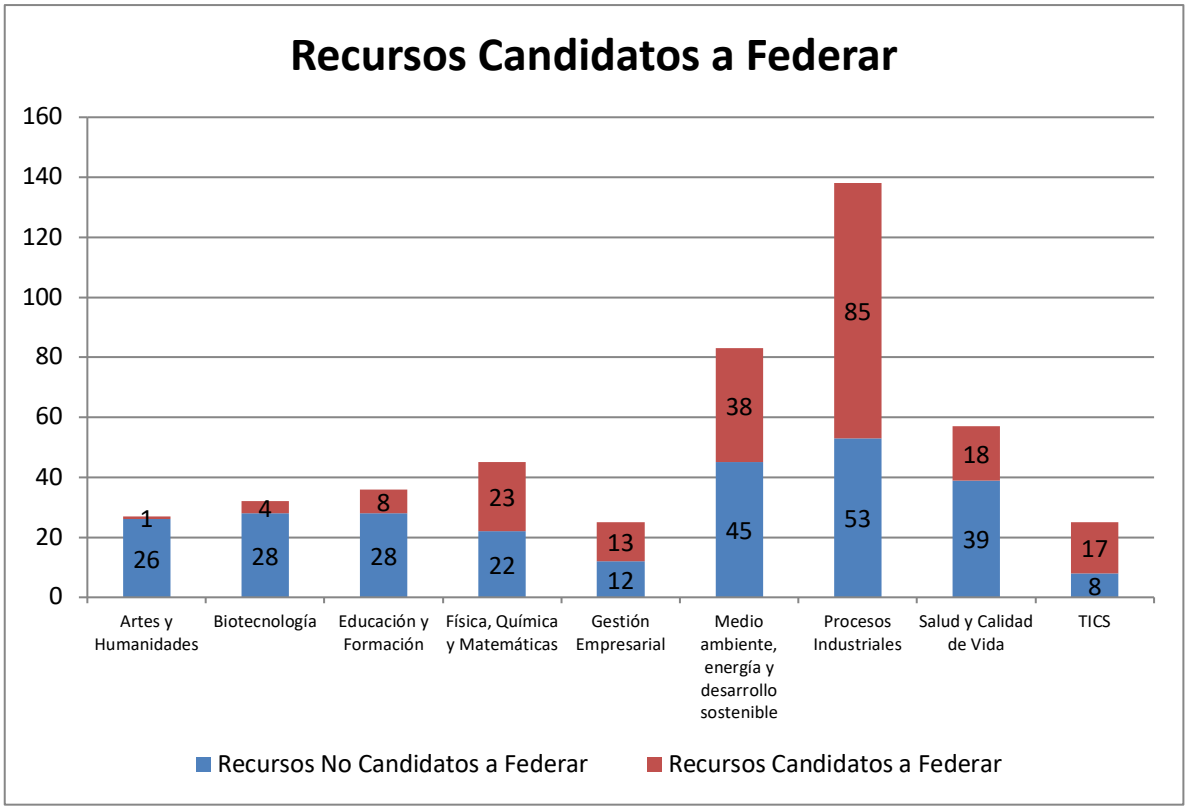



***Ilustración 13*** *Recursos candidatos a Federar por Área de interés*[14]

De la totalidad de 464 recursos identificados, se han seleccionado 207 como candidatos a ser Servicios federados tomando como criterio que sean recursos computacionales, equipos, software y prototipos. (Ver **Ilustración 13**)

[14] **Fuente:** Del autor

### *5.1.2.7 Recursos candidatos a federar computacionales*

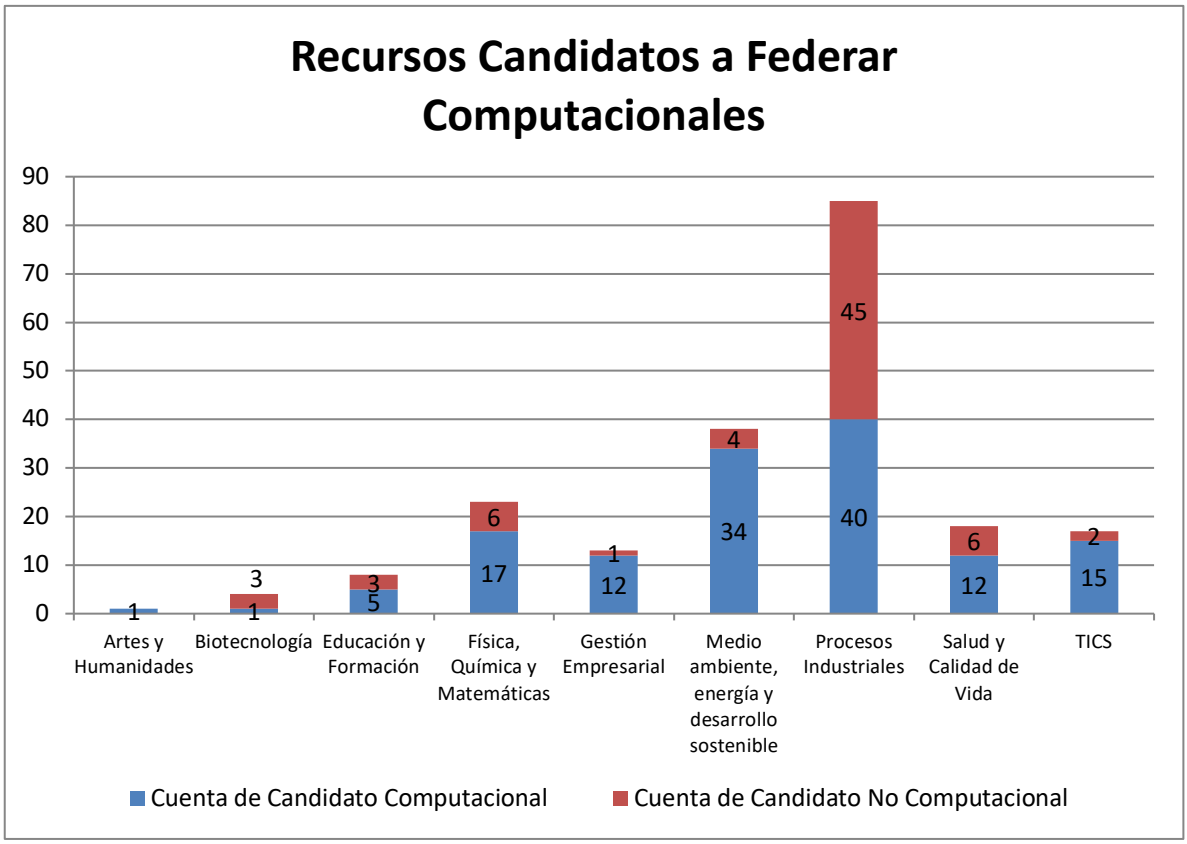



***Ilustración 14*** *Recursos candidatos a federar computacionales*[15]

De los 207 recursos candidatos a federar, 137 son recursos computacionales o software. Este tipo de capacidades facilitan su federación. Cabe resaltar que aunque "TICS" y "Gestión Empresarial" tienen pocos recursos identificados, la mayoría son computacionales (Ver **Ilustración 14**).

[15] **Fuente:** Del autor

### *5.1.2.8 Capacidades computacionales por Área de investigación*

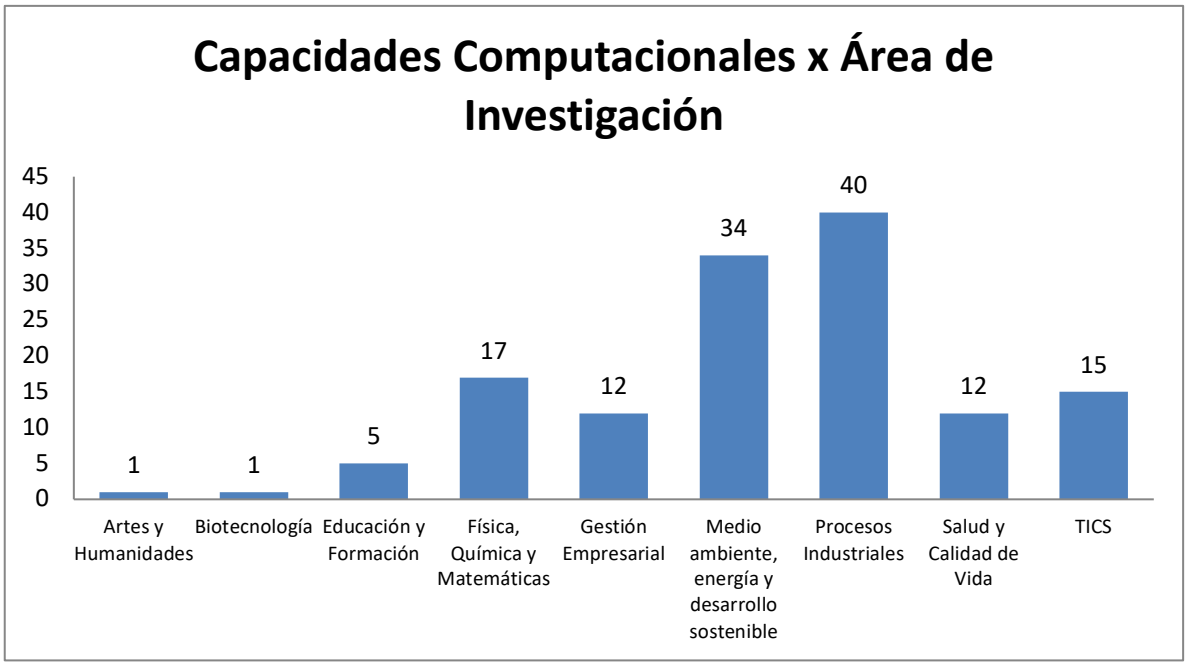



***Ilustración 15*** *Capacidades computacionales por Área de investigación*[16]

En la **Ilustración 15** se puede notar que la mayor cantidad de recursos computaciones se encuentran registrados bajo el área de interés "Procesos Industriales", seguido por "Medio Ambiente, Energía y Desarrollo Sostenible" como se puede identificar también en la **Ilustración 16**

[16] **Fuente:** Del autor

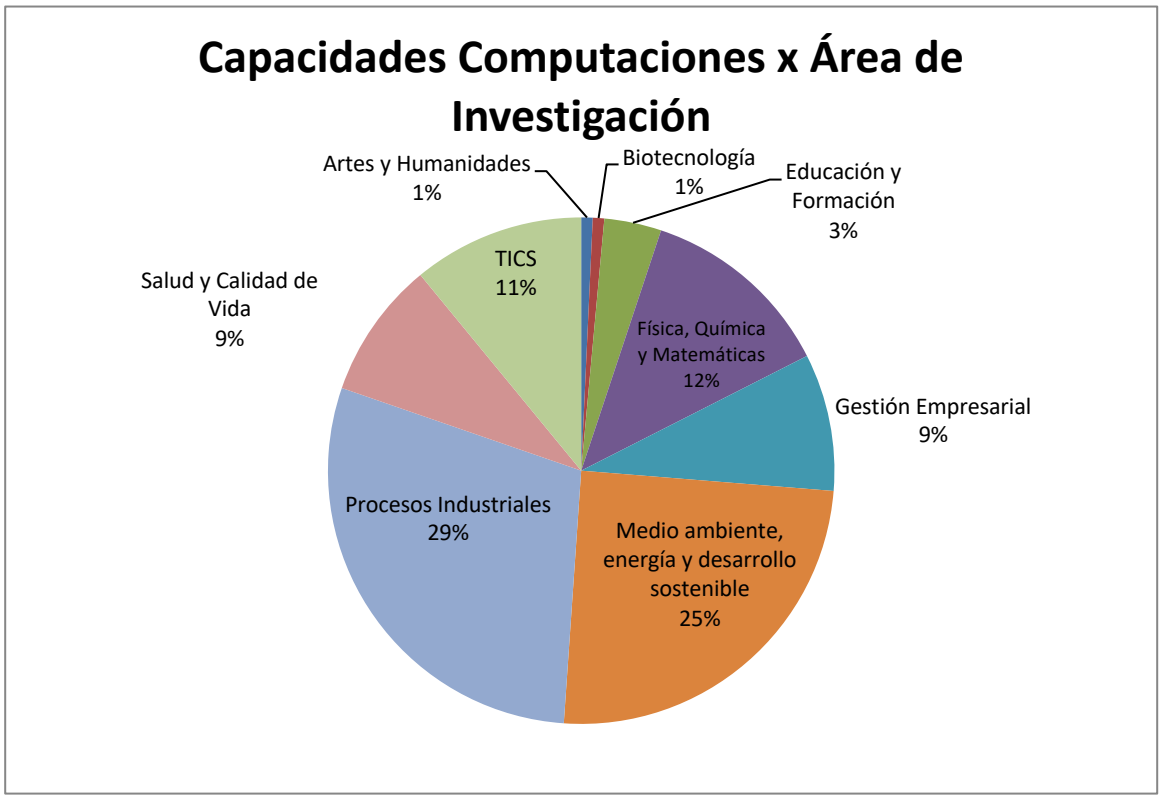



***Ilustración 16*** *Capacidades computacionales por área de investigación (%)*[17]

### *5.1.2.9 Listado de recursos computacionales por área de interés*

a. Artes y Humanidades.

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Artes y Humanidades** | Grupo de investigación L'H | Software: Multimedia : Facultad de producción en Artes Audiovisuales. Colombia, 2006, Disponibilidad: Irrestricta, Institución financiadora: Autores: SEAN IGOR ACOSTA DIAZ, |

***Tabla 1*** *Recursos computacionales – Artes y Humanidades*

b. Biotecnología

[17] **Fuente:** Del autor

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Biotecnología** | Grupo de investigación agua y saneamiento GIAS | Desarrollo de software: especializado para catastro de redes de agua potable y aguas residuales |

***Tabla 2*** *Recursos computacionales - Biotecnología*

c. Educación y Formación

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Educación y Formación** | Estudios Metodológicos para la Enseñanza de la Matemática y el uso de las Nuevas Tecnologías de la Información y la Comunicación - EMEMATIC | ALTIC - software para dictar curso de álgebra lineal |
| | | Software MATHTIC (Está en desarrollo) |
| | Grupo de investigación Educación y Desarrollo Humano | Computacional: Diseño del curso de Pedagogía en la Virtualidad en la plataforma Moodle Colombia, 2007, Disponibilidad: Restringido, Sitio web: http://univirtual.utp.edu.co/aula/ |
| | | Cursos y seminarios tal como: Computacional : Diseño del curso de Pedagogía en la Virtualidad en la plataforma Moodle Colombia, 2007, Disponibilidad: Restringido, Sitio web: http://univirtual.utp.edu.co/aula/ |
| | Grupo de investigación en lingüística aplicada a la enseñanza de las lenguas -Poliglosia | Página web : http://dollytam.wixsite.com/poliglosialbi. Poliglosia. Grupo de investigación en lingüística aplicada a la enseñanza de las lenguas 2016-08-01, Entidades vinculadas: Universidad tecnológica de Pereira a través de la licenciatura en bilingüismo con énfasis en ingles por medio de Poliglosia-Grupo de investigación en lingüística aplicada a la enseñanza de las lenguas. Autores: DOLLY RAMOS GALLEGO, |

***Tabla 3*** *Recursos computacionales – Educación y Formación*

d. Física, Química y Matemáticas

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Física, Química y Matemáticas** | Grupo de investigación ecuaciones diferenciales y aplicaciones - GREDYA | 1.- Computacional : PBairstow<br>Colombia, 2015, Disponibilidad: Restringido, Sitio web:<br>Nombre comercial: PBairstow, Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: JORGE EDUARDO OSSA SANCHEZ, DIANA PAOLA MEJIA ROJAS, DIEGO FERNANDO DEVIA NARVAEZ, |
| | | 2.- Computacional : PREGLAFALSA<br>Colombia, 2014, Disponibilidad: Restringido, Sitio web:<br>Nombre comercial: PReglaFalsa, Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: JORGE EDUARDO OSSA SANCHEZ, |
| | | 3.- Computacional : EF.dll<br>Colombia, 2014, Disponibilidad: Restringido, Sitio web:<br>Nombre comercial: EF.dll, Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: JORGE EDUARDO OSSA SANCHEZ, DIEGO FERNANDO DEVIA NARVAEZ, DIANA PAOLA MEJIA ROJAS, |
| | | 4.- Computacional : PBISECCION<br>Colombia, 2013, Disponibilidad: Restringido, Sitio web:<br>Nombre comercial: , Nombre del proyecto: |
| | Grupo de Investigación en Astroingeniería Alfa Orión | Software Computacional : AstroCorr<br>Colombia, 2013, Disponibilidad: Restringido, Sitio web: http://observatorioastronomico.utp.edu.co/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, ANA CAROLINA ACUNA ESCOBAR, MAURIO HOLGUIN LONDONO, |
| | | Software Computacional : AstroDiff<br>Colombia, 2011, Disponibilidad: No restringido, Sitio web: http://observatorioastronomico.utp.edu.co/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, MAURIO HOLGUIN LONDONO, WILLIAM ARDILA URUENA |
| | | Software Computacional : DIFIAC v. 1.0<br>Colombia, 2012, Disponibilidad: Restringido, Sitio web: http://observatorioastronomico.utp.edu.co/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, ARLEY BEJARANO MARTINEZ, MAURIO HOLGUIN LONDONO, |
| | | Software Computacional : LAMBDA FOR LHIRES III<br>Colombia, 2017.<br>Autores: IVAN DARIO ARELLANO RAMIREZ, ANGELICA MARIA GUAPACHA, JAIRO ALBERTO AGUIRRE GALVIS, |
| | | Software Computacional : Minimizado Global de Funciones de Computación<br>Colombia, 2010, Disponibilidad: Restringido, Sitio web: http://observatorioastronomico.utp.edu.co/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, ANDRES ESCOBAR MEJIA, MAURIO HOLGUIN LONDONO, |
| | | Software Computacional : NetMatrix<br>Colombia, 2012, Disponibilidad: Restringido, Sitio web: https://sites.google.com/a/utp.edu.co/netmatrix-toolbox/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, TOMAS ECHEVERRI VALENCIA, MAURIO HOLGUIN LONDONO, |
| | | Software Computacional : Simulador Comportamental para Cruce Semafórico<br>Colombia, 2012, Disponibilidad: Restringido, Sitio web: http://observatorioastronomico.utp.edu.co/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, ALVARO ANGEL OROZCO GUTIERREZ, MAURIO HOLGUIN LONDONO, |
| | | Software Computacional : SINTAF<br>Colombia, 2010, Disponibilidad: Restringido, Sitio web: http://observatorioastronomico.utp.edu.co/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, ALVARO ANGEL OROZCO GUTIERREZ, MAURIO HOLGUIN LONDONO, |
| | | Software Computacional : SoftBull v. 1.0<br>Colombia, 2012, Disponibilidad: Restringido, Sitio web: http://observatorioastronomico.utp.edu.co/<br>Autores: EDWIN ANDRES QUINTERO SALAZAR, GERMAN ANDRES HOLGUIN LONDONO, MAURIO HOLGUIN LONDONO, |
| | Grupo de investigación en ecuaciones diferenciales no lineales - GEDNOL | Programas computacionales: SERVIADMIN, SERVIMATH, SERVITOOLS, SERVISIÓN, SERVINVENTARIO, SERVICONTROL, SERVIBIBLIOTECA, SERVIAUDITOR, ServiCalidad, WebServi, ServiOptica, ServiMedic, ServiSigtel, ServiCursos. |
| | Grupo de Investigación en propiedades magnéticas y magneto-ópticas de nuevos | Software cuantificación de efectos superficiales y subsuperficiales en materiales (polímeros) |
| | Grupo de Investigación Geometría y algebra - GIGA | Software: MATHTIC<br>Autores: Julio Vargas - Vivian Uzuriaga Lopez |
| | Grupo de Investigación Gravitación y teorías unificadas | Clúster computacional<br>Laboratorio de Investigaciones Fundamentales |

***Tabla 4*** *Recursos computacionales – Física, Química y Matemáticas*

e. Gestión Empresarial

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Gestión Empresarial** | Grupo de investigación Aplicaciones de técnicas de optimización y procesos estocásticos - GAOPE - | Computacional : AsignaTASK V1.0<br>Colombia, 2005, Disponibilidad: Irrestricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: ELIANA MIRLEDY TORO OCAMPO, RAMON ALFONSO GALLEGO RENDON, MAURICIO GRANADA ECHEVERRI, |
| | | Computacional : Simular SR<br>Colombia, 2004, Disponibilidad: Irrestricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora:<br>Autores: ALEJANDRO GARCES RUIZ, JUAN CARLOS GALVIS MANZO, |
| | | Computacional : TrifaSYS V.1.0<br>Colombia, 2005, Disponibilidad: , Sitio web:<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: ALEJANDRO GARCES RUIZ, |
| | | Multimedia : PANDORA<br>Colombia, 2011, Disponibilidad: Restringido, Sitio web:<br>http://univirtual.utp.edu.co/pandora/scripts/login/entrar.php |
| | Grupo de investigación Productividad y competitividad en las organizaciones -GIPCO- | Software Estadístico |
| | Grupo Estudio y aplicación de herramientas estadísticas modernas en la solución de problemas del entorno-GIEM | Computacional : Sistema de competencias lectoras. Colombia, 2013, Disponibilidad: Restringido, Sitio web: http://www.investigarlambda.com/demos<br>Autores: PATRICIA CARVAJAL OLAYA, |
| | | Computacional : Sistema de competencias Matemáticas<br>Colombia, 2013, Disponibilidad: Restringido, Sitio web:<br>http://www.investigarlambda.com/demos<br>Nombre comercial: Sistema de competencias Matemáticas, Nombre del proyecto:<br>Institución financiadora: investigarlambda sas<br>Autores: PATRICIA CARVAJAL OLAYA, |
| | | Software Computacional : Sistema de Orientación Profesional. Colombia, 2013.<br>Institución financiadora: investigarlambda sas<br>Autores: PATRICIA CARVAJAL OLAYA, |
| | | Software Computacional : Sistema de valoración de competencias: Prueba de conocimientos matemáticos y Prueba de comprensión lectora, Colombia, 2011, Sitio web:<br>http://arquimedes.utp.edu.co/observatorio/softpruebas/pruebasvaloracion/<br>Autores: ALVARO ANTONIO TREJOS CARPINTERO, |
| | | Software Computacional : SISTEMA DE VALORACION DE RIESGO PARA LA DESERCION, SALUD FÍSICA Y MENTAL, ENTREVISTA DE INGRESO Y PRUEBA DE MOTIVACIÓN. Colombia, 2011,Sitio web:<br>http://arquimedes.utp.edu.co/observatorio/softpruebas/pruebasvaloracion/<br>Autores: ALVARO ANTONIO TREJOS CARPINTERO, |
| | | Software Computacional : Sistema Integrado de Alertas Tempranas - Colombia, 2013, Sitio web: http://www.investigarlambda.com/demos/satv5/<br>Autores: PATRICIA CARVAJAL OLAYA, |
| | | Servidores computacionales de alta capacidad |

***Tabla 5*** *Recursos computacionales – Gestión Empresarial*

f. Medio Ambiente, Energía y Desarrollo

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Medio ambiente, energía y desarrollo sostenible** | Gestión de Sistemas Eléctricos Electrónicos y Automáticos | Computacional : DITRAM. Colombia, 2015.<br>Autores: MAURICIO HOLGUIN LONDONO, JESSER JAMES MARULANDA DURANGO, ANDRES ESCOBAR MEJIA, |
| | | Diseño y construcción de un contador de pasajeros de buses públicos utilizando video cámaras y sistemas embebidos. Colombia, 2016.<br>Institución que se benefició del servicio: LOGIRASTREO S.A.S<br>Autores: LEIDY ESPERANZA PAMPLONA BERON, ANDRES FELIPE CALVO SALCEDO, ARLEY BEJARANO MARTINEZ |
| | | Software Computacional : CACONT. Colombia, 2016.<br>Autores: MAURICIO HOLGUIN LONDONO, ALFONSO ALZATE GOMEZ, JESSER JAMES MARULANDA |
| | | Software Computacional : CONVCC. Colombia, 2015<br>Autores: MAURICIO HOLGUIN LONDONO, JESSER JAMES MARULANDA DURANGO, ALFONSO ALZATE GOMEZ, |
| | | Software Computacional : EPMI. Colombia, 2015.<br>Autores: MAURICIO HOLGUIN LONDONO, ANDRES ESCOBAR MEJIA, JESSER JAMES MARULANDA DURANGO, |
| | | Software Computacional : MONOMORF. Colombia, 2016.<br>Autores: GERMAN ANDRES HOLGUIN LONDONO, MAURICIO HOLGUIN LONDONO, ANDRES ESCOBAR MEJIA,DURANGO,ALVAREZ LOPEZ |
| | | Software Computacional : Optinet. Colombia, 2016.<br>Autores: MAURICIO HOLGUIN LONDONO, ALVARO ANGEL OROZCO GUTIERREZ, MAURICIO ALEXANDER |
| | | Software Computacional : SICOCONV. Colombia, 2015<br>Autores: JESSER JAMES MARULANDA DURANGO, MAURICIO HOLGUIN LONDONO, |
| | | Software Computacional : SICOTANK. Colombia, 2015<br>Autores: JESSER JAMES MARULANDA DURANGO, MAURICIO HOLGUIN LONDONO, |
| | | Software Computacional : SINTLOGIC. Colombia, 2013,<br>Autores: GERMAN ANDRES HOLGUIN LONDONO, MAURICIO HOLGUIN LONDONO, JESSER JAMES MARULANDA DURANGO, |
| | | Software Computacional : SYMACOS. Colombia, 2016.<br>Autores: ANDRES ESCOBAR, GERMAN ANDRES HOLGUIN LONDONO, WALTER JULIAN GIL GONZALEZ, |
| | Investigación en conceptos emergentes de energía eléctrica ICE3 | FINDER<br>Software para localización de fallas en Redes Eléctricas |
| | Laboratorio de investigación en desarrollo eléctrico y electrónico - LIDER | Software para la identificación de usuarios infractores, DISCOVER |

***Tabla 6*** *Recursos computacionales – Medio Ambiente, Energía y Desarrollo Sostenible (Parte 1)*

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Medio ambiente, energía y desarrollo sostenible** | Planeamiento en Sistemas Eléctricos | Computacional : Asignación óptima de tareas – AsignaTASK V 1.0. Colombia, 2005, Investigación y simulación de fenómenos.<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, ELIANA MIRLEDY TORO OCAMPO, |
| | | Computacional : Distribución MC. Colombia, 2005.<br>Autores: OSCAR GOMEZ CARMONA, |
| | | Computacional : LORDS – Losses Reduction in Distribution System – versión trifásica. Colombia, 2007<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, ALEJANDRO GARCES RUIZ, |
| | | Computacional : TRIFASYS – FLUJO DE POTENCIA TRIFASICO<br>Colombia, 2006, , Irrestricta, PC, Windows, , , Investigación y simulación de sistemas eléctricos. |
| | | Computacional : Análisis de sistemas de Potencia V. 1.0 Colombia, 2005, Simulación de fenómenos.<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, JUAN JOSE MORA FLORES, |
| | | Computacional : ANALISIS DE SISTEMAS DE POTENCIA V1.0 Colombia, 2005. Simulación de sistemas eléctricos. Autores: RAMON ALFONSO GALLEGO RENDON, MAURICIO GRANADA ECHEVERRI, JUAN JOSE MORA FLOREZ, |
| | | Computacional : AsignaTASK V 1.0 Colombia, 2005, Asigna TASK, Irrestricta, PC, Windows, , , Investigación y simulación de fenómenos. Autores: MAURICIO GRANADA ECHEVERRI, ELIANA MIRLEDY TORO OCAMPO, RAMON ALFONSO GALLEGO RENDON, |
| | | Computacional : Flujo de potencia trifásico – TrifaSYS V.1.0 Colombia, 2005, Investigación y simulación de fenómenos. |
| | | Computacional : Modelo de Estimación del Costo Total del Plan de Reducción de Pérdidas No Técnicas Colombia, 2011, Convenio Interadministrativo UTP-CREG 2010-0137, Comisión de Regulación de Energía y Gas, Programa que calcula el costo óptimo de un plan de disminución de pérdidas no técnicas.<br>Autores: HAROLD SALAZAR ISAZA, CAMILO A GALLEGO, JOSE A. JARAMILLO VILLEGAS, RENE GOMEZ LONDONO, JHON H. OSORIO RIOS, |
| | | Computacional : Sistema de información audifarma Colombia, 2002,<br>Autores: MAURICIO GRANADA ECHEVERRI, |

***Tabla 7*** *Recursos computacionales – Medio Ambiente, Energía y Desarrollo Sostenible (Parte 2)*

g. Procesos Industriales

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Procesos Industriales** | Gestión de Sistemas Eléctricos Electrónicos y Automáticos | Computacional : DITRAM. Colombia, 2015.<br>Autores: MAURICIO HOLGUIN LONDONO, JESSER JAMES MARULANDA DURANGO, ANDRES ESCOBAR MEJIA, |
| | | Software Computacional : CACONT. Colombia, 2016.<br>Autores: MAURICIO HOLGUIN LONDONO, ALFONSO ALZATE GOMEZ, JESSER JAMES MARULANDA |
| | | Software Computacional : CONVCC. Colombia, 2015<br>Autores: MAURICIO HOLGUIN LONDONO, JESSER JAMES MARULANDA DURANGO, ALFONSO ALZATE GOMEZ, |
| | | Software Computacional : EPMI. Colombia, 2015.<br>Autores: MAURICIO HOLGUIN LONDONO, ANDRES ESCOBAR MEJIA, JESSER JAMES MARULANDA DURANGO, |
| | | Software Computacional : MONOMORF. Colombia, 2016.<br>Autores: GERMAN ANDRES HOLGUIN LONDONO, MAURICIO HOLGUIN LONDONO, ANDRES ESCOBAR MEJIA,DURANGO,ALVAREZ LOPEZ |
| | | Software Computacional : Optinet. Colombia, 2016.<br>Autores: MAURICIO HOLGUIN LONDONO, ALVARO ANGEL OROZCO GUTIERREZ, MAURICIO ALEXANDER |
| | | Software Computacional : SICOCONV. Colombia, 2015<br>Autores: JESSER JAMES MARULANDA DURANGO, MAURICIO HOLGUIN LONDONO, |
| | | Software Computacional : SICOTANK. Colombia, 2015<br>Autores: JESSER JAMES MARULANDA DURANGO, MAURICIO HOLGUIN LONDONO, |
| | | Software Computacional : SINTLOGIC. Colombia, 2013,<br>Autores: GERMAN ANDRES HOLGUIN LONDONO, MAURICIO HOLGUIN LONDONO, JESSER JAMES MARULANDA DURANGO, |
| | | Software Computacional : SYMACOS. Colombia, 2016.<br>Autores: ANDRES ESCOBAR, GERMAN ANDRES HOLGUIN LONDONO, WALTER JULIAN GIL GONZALEZ, |

***Tabla 8*** *Recursos computacionales – Procesos Industriales (Parte 1)*

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Procesos Industriales** | Grupo de Investigación Desarrollo en investigación de operaciones -DINOP- | Computacional : Análisis de sistemas de Potencia V. 1.0<br>Colombia, 2005, Disponibilidad: No restringido, Sitio web: www.utp.edu.co<br>Nombre comercial: Análisis de sistemas de Potencia V. 1.0, Nombre del proyecto: resolución CIARP<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, JUAN JOSE MORA FLORES, |
| | | Computacional : Asignación óptima de tareas - AsignaTASK V 1.0<br>Colombia, 2005, Disponibilidad: Irrestricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, ELIANA MIRLEDY TORO OCAMPO |
| | | Computacional : AsignaTASK V 1.0<br>Colombia, 2005, Disponibilidad: Irrestricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, ELIANA MIRLEDY TORO OCAMPO, |
| | | Computacional : Distribución MC<br>Colombia, 2005, Disponibilidad: Irrestricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto: |
| | | Computacional : Flujo de potencia trifásico - TrifaSYS V.1.0<br>Colombia, 2005, Disponibilidad: Irrestricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp |
| | | Computacional : LORDS - Losses Reducción in Distribución Sistema - versión trifásica<br>Colombia, 2007, Disponibilidad: Restricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto: Resolución No 126-0309-00<br>Institución financiadora: Universidad Tecnológica de Pereira - COLCIENCIAS<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, ALEJANDRO GARCES RUIZ. |
| | | Computacional : Sistema de información audifarma Colombia, 2002, Disponibilidad: Restricta, Sitio web: http://www.audifarma.com.co<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora: Audifarma S.A.<br>Autores: MAURICIO GRANADA ECHEVERRI, |
| | | Computacional : TrifaSYS V.1.0<br>Colombia, 2005, Disponibilidad: Irrestricta, Sitio web:<br>Nombre comercial: , Nombre del proyecto:<br>Institución financiadora: Universidad Tecnológica De Pereira - Utp<br>Autores: MAURICIO GRANADA ECHEVERRI, RAMON ALFONSO GALLEGO RENDON, ALEJANDRO GARCES RUIZ, |

***Tabla 9*** *Recursos computacionales – Procesos Industriales (Parte 2)*

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Procesos Industriales** | Grupo de Investigación Electrónica de potencia | Computacional : CACont<br>Colombia, 2016<br>Autores: JESSER JAMES MARULANDA DURANGO, ALFONSO ALZATE GOMEZ, MAURICIO HOLGUIN LONDONO, |
| | | Computacional : CONVCC<br>Colombia, 2015<br>Autores: JESSER JAMES MARULANDA DURANGO, ALFONSO ALZATE GOMEZ, MAURICIO HOLGUIN LONDONO |
| | | Computacional : DITRAM<br>Colombia, 2015<br>Autores: ANDRES ESCOBAR MEJIA, MAURICIO HOLGUIN, JAMES MARULANDA, |
| | | Computacional : EPMI<br>Colombia, 2015<br>Autores: ANDRES ESCOBAR MEJIA, JAMES MARULANDA, MAURICIO HOLGUIN, |
| | | Computacional : MONOMORF (2016)<br>Autores: ANDRES ESCOBAR MEJIA, GERMAN ANDRES HOLGUIN, MAURICIO HOLGUIN, |
| | | Computacional : PWMCLICK<br>Colombia, 2013<br>Autores: ALFONSO ALZATE GOMEZ, JESSER JAMES MARULANDA DURANGO, MAURICIO HOLGUIN LONDONO |
| | | Computacional : SYMACOS (2016)<br>Autores: ANDRES ESCOBAR MEJIA |
| | Grupo de investigación en Automática | Computadores avanzados, Bases de datos actualizadas |
| | Grupo de Investigación en Conformado de Materiales Metálicos - CONFORMAT | Software para la selección de correas trapezoidales |
| | | En la UTP: Equipo de cómputo especializado para simulación, Microcopio óptico, Equipos de preparación metalográfica, Máquina universal, Hornos tipo mufla para tratamientos térmicos, y Microdurometro Vickers y Knoop, durometros Vickers, Rockwell y Brinell. En la Uniatlantico: Equipo de cómputo especializado para simulación, Hornos tipo mufla para tratamientos térmicos, matrices para técnicas de deformación plástica, RUGOSÍMETRO DIGITAL MARCA FISCHER DUALSCOPE® FMP20, BAÑO ULTRASÓNICO DE 1.75 L MARCA PRESI, BALANZA ANALÍTICA ME-T ME204T , Durómetro Digital Portátil Dispositivo de impacto D. Incluidora metalográfica de probetas, Cortadora de presición, Pulidora metalográfica de disco, Microscopio óptico, Máquina universal de ensayos, Equipo para ensayos de fatiga por flexión rotativa y Equipos para la evaluación de la resistencia al desgaste adhesivo y abrasivo segun normas ASTM G83, G65, G99, G76 |

***Tabla 10*** *Recursos computacionales – Procesos Industriales (Parte 3)*

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Procesos Industriales** | Grupo de investigación en Control Automático | Software Computacional : Análisis de Variabilidad de Señales Cardiovasculares (2009), Disponibilidad: No restringido<br>Autores: EDUARDO GIRALDO SUAREZ |
| | | Software Computacional : CALCULO DE REDES SECUNDARIAS (2009), Disponibilidad: Restringido<br>Autores: EDUARDO GIRALDO SUAREZ |
| | | Software Computacional : Identificacion y control de sistemas (2016), Disponibilidad: Restringido,<br>Autores: EDUARDO GIRALDO SUAREZ |
| | | Software Computacional : Regulación de Redes Secundarias en Topologías Radiales y con Anillos (2012), Disponibilidad: Restringido<br>Autores: EDUARDO GIRALDO SUAREZ |
| | | Disponibilidad: Restringido<br>Autores: EDUARDO GIRALDO SUAREZ |
| | Grupo de Investigación en Procesos de Manufactura y Diseño de Máquinas | Herramientas computacionales (SolidWorkds, ANSYS), máquina de prototipado rápida, máquina CNC, laboratorio de resitencia materiales, sistemas dinámicos y control, laboratorio de vibraciones |
| | Grupo de Investigación en robótica y percepción sensorial - GIROPS - | Robots desarrollados |
| | Grupo de investigación Robótica Aplicada | Computacional : SIRUM - SIMULADOR DE ESCENARIOS PARA LA BÚSQUEDA DE RUTAS EN ROBÓTICA MÓVIL (2012)<br>AUTOR: JOSE ANDRES CHAVES OSORIO |
| | | Computacional : VisioPen - Software para el estudio del movimiento armónico simple del péndulo simple (2013),<br>Autores: JIMY ALEXANDER CORTES OSORIO, JOSE ANDRES CHAVES OSORIO, JAIRO ALBERTO MENDOZA VARGAS |
| | Planeamiento en Sistemas Eléctricos | Computacional : Distribución MC. Colombia, 2005.<br>Autores: OSCAR GOMEZ CARMONA, |
| | TransFórmate | Software Computacional : INNOBUS B2B. Colombia, 2012.<br>Plataforma que ha ido creciendo a partir de varios módulos, se agregan a las tesis |
| | | Servidores SITE y de la empresa, máquinas de 20 núcleos, acceso a datos de operación de los últimos 7 años del sistema |

***Tabla 11*** *Recursos computacionales – Procesos Industriales (Parte 4)*

h. Salud y Calidad de Vida

| Etiquetas de fila | Nombre del grupo | Capacidades |
|---|---|---|
| **Salud y Calidad de Vida** | Grupo de investigación en Básico-Clínica y Aplicadas | Software Computacional : VitalApp Sitio web: http://vital-app.com/ 2016 Nombre comercial: VitalApp |
| | | Software Computacional : Monitoreo de variables físicas y fisiológicas en niños y adolescentes en edad escolar en el departamento de Risaralda de la Universidad Tecnológica de Pereira, Colombia, 2013 Sitio web: salud.grande.com.co Nombre comercial: SOFTWARE DE MONITOREO para identificar las fortalezas y debilidades de niños con miras a enfocarlos en deportes específicos - historia clínica de acuerdo a los parámetros ingresados |
| | Grupo de Investigación en Gerencia de Sistemas de Salud | Página web : OBSERVATORIO DE POLITICAS DE INFANCIA Y HUVENTUD OPIJ (2014-12-26), Sitio web: www.observatorioinfancia.com , Autores: PATRICIA GRANADA ECHEVERRI, |
| | | Software Computacional : Garantía Ciudades Inteligentes para la Infancia V1 : brinda información de los niños para ciudades saludables (2014), Sitio web: www.garantya.co, Autores: LUZ ANGELA CARDONA ARCE, DIOMEDES TABIMA GARCIA, PATRICIA GRANADA ECHEVERRI |
| | | Software Computacional : PLATAFORMA DE LINEA BASE DEL SISTEMA DE INFORMACION DE INFANCIA, PARA SER UTILIZADO EN LOS CDI DE ICBF (2014) Autores: DIOMEDES TABIMA GARCIA |
| | | Software Computacional : SISPEA (2014), Disponibilidad: Restringido, Sitio web: www.sispea.com/ese-pereira/public, Autores: JUAN CARLOS OLARTE CORTES |
| | Grupo de Investigación Epidemiología, salud y violencia | Software, regresión LOESS |
| | Grupo de Investigación estadística y epidemiología - GIEE- | Computacional : La Física en el Corazón (Colombia, 2012) Institución financiadora: FUAA Autores: JOSE GERARDO CARDONA TORO, LUZ MARIA ROJAS DUQUE, GABRIEL ISAZA SEPULVEDA, |
| | | Gen Clonado : Software para el análisis del rendimiento del futbolista (Colombia, 2012) Autores: JOSE GERARDO CARDONA TORO, |
| | Grupo de Investigación Salud pública e infección | Software especializado, para el análisis de datos y georeferenciación. |
| | Grupo de Investigación y desarrollo en la cultura de la salud | Software Computacional : Garantya Ciudades Inteligentes para la Infancia V1, Colombia, 2014, Sitio web: www.garantya.co . Autores: LUZ ANGELA CARDONA ARCE, DIOMEDES TABIMA GARCIA, PATRICIA GRANADA ECHEVERRY |
| | | Software Computacional : SISTEMA DE INFORMACIÓN GEORREFERENCIADO DE INFANCIA Y JUVENTUD Colombia, 2011, Sitio web: www.opij.org , Nombre comercial: INFANCIA EN RED. Autores: PATRICIA GRANADA ECHEVERRI, ALEXANDER ROZO PATIÑO. |

***Tabla 12*** *Recursos computacionales – Salud y Calidad de Vida*

i. TICs

| Etiquetas de fil | Nombre del grupo | Capacidades |
|---|---|---|
| **TICS** | Grupo de avanzada en desarrollo de software -GRANDE- | Desarrollo de una plataforma web para ayudar a las empresas a desarrollar software eficientemente |
| | | Computadores avanzados |
| | Grupo de InvestigciónTelecomunicaciones NYQUIST | Computacional : SOFTWARE PARA CONTROL DE ENTRADA Y SALIDA DE VEHICULOS MEDIANTE REDES INALAMBRICAS, Colombia, 2008<br>Autores: ANA MARIA LOPEZ ECHEVERRY, |
| | | Computacional : DEFINICIÓN DE PROCESOS DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SOPORTADO EN TIC'S, Colombia, 2011<br>Autores: ANA MARIA LOPEZ ECHEVERRY, PAULA ANDREA VILLA SANCHEZ, |
| | | Computacional : MÓDULO DE GESTIÓN DE AUDITORÍA SOPORTADO EN TIC PARA LA GESTIÓN DE COMUNICACIONES, SEGUIMIENTO Y REVISIÓN DEL SGSI, Colombia, 2014,<br>Autores: EDWARD FABIAN PENAGOS GRANADA, ANA MARIA LOPEZ ECHEVERRY |
| | | Computacional : SOFTWARE PARA DOCUMENTACION DE REDES DE COMUNICACIÓN, Colombia, 2008<br>Autores: ANA MARIA LOPEZ ECHEVERRY |
| | | Computacional: MIGEN, Colombia, 2006<br>Autores: SAULO DE JESUS TORRES RENGIFO, ANDREA GALLEGO, DIANA ISIS DAVILA, PAULA ANDREA CORTES |
| | Grupo Sirius | Computacional : CVTraffic 2014<br>Colombia, 2016,<br>Autores: ESTEBAN CORREA AGUDELO, JUAN DAVID HINCAPIE, DIEGO AGUDELO, JUAN DAVID GIL, JHON BERNARDO JIMENEZ |
| | | Computacional : Encuesta Matriz Origen Destino<br>Colombia, 2015,<br>Autores: ORLANDO ANTONIO SABOGAL CARDONA, |
| | | Computacional : GAUSS SIMULATION RT<br>Colombia, 2015, Nombre comercial: GAUSS SIMULATION RT<br>Autores: DAVID ALEJANDRO JIMENEZ OSORIO, JUAN DAVID HINCAPIE ZEA, JUAN MANUEL AMARILES ZAMBRANO, DAVID ALBEIRO TABORDA ALVAREZ, |
| | | Computacional : GAUSS<br>Colombia, 2015,<br>Autores: DAVID ALEJANDRO JIMENEZ OSORIO, JUAN DAVID HINCAPIE ZEA, FABIAN LEANDRO MUNOZ TOBON, JUAN SEBASTIAN ARIAS HERNANDEZ, |
| | | Computacional : LINEAS DE DESEO<br>Colombia, 2014,<br>Autores: ORLANDO ANTONIO SABOGAL CARDONA, |
| | | Computacional : MODELO DE ESCALDA MULTIMENSIONAL<br>Colombia, 2014,<br>Autores: ORLANDO ANTONIO SABOGAL CARDONA, |
| | | Computacional : Oportunidades Acumuladas<br>Colombia, 2015,<br>Autores: ORLANDO ANTONIO SABOGAL CARDONA, |
| | | 17 equipos de computo de alto desempeño, Laboratorio de fotonica, Laboratorios Sirius HPC y Laboratorio Sirius ITS |

***Tabla 13*** *Recursos computacionales - TICs*

### 5.1.3 Resumen de los problemas, oportunidades y necesidades

**Problemas**

- Ejecución presupuestal atomizada, distribuidos entre facultades, grupos de investigación e investigadores.
- Existencia de recursos costosos que no se comparten entre grupos de investigación.
- Recursos existentes con capacidades computacionales desaprovechadas.

**Necesidades**

- Aprovechar mejor los recursos existentes.
- Dar a conocer las capacidades de los grupos de investigación.
- Orientar inversiones en adquisición tecnológica.

**Oportunidades**

- De las capacidades recolectadas en los grupos de investigación objeto de este estudio se identificaron 207 recursos candidatos a federar, de los cuales 137 son recursos computacionales o software.

## 5.2 TECNOLOGÍAS PARA FEDERACIÓN DE IDENTIDAD

Esta sección se desarrolla con el propósito de identificar tecnologías que permitan a través de su implementación, presentar una solución a los problemas, necesidades y oportunidades encontradas en el desarrollo de este proyecto.

Contar con la tecnología para brindar acceso a un conjunto de recursos, ayuda a solucionar los problemas realcionados con la ejecución presupuestal atomizada, aprovechar capacidades computacionales existentes, además de favorecer el uso de estos recursos entre diferentes grupos de investigación. Por lo anterior es posible focalizar los presupuestos hacia la adquisición de recursos que brinden una mayor entrega de valor para la UTP.

Las oportunidades consideradas en este trabajo están relacionadas con las capacidades identificadas de los grupos de investigación según el estudio realizado por la vicerrectoría de investigaciones. En los grupos de investigación existen recursos que pueden ser compartidos a la comunidad académica interna o externa, y en este sentido la selección de la tecnología adecuada para la federación de estos recursos facilita su visualización y acceso.

Los principales estándares para implementar federación de identidad que se están utilizando actualmente son OAUTH 2.0, OPENID CONNECT y SAML (Wilson,

Hingnikar, Wilson, & Hingnikar, 2019). Por lo anterior, en las secciones siguientes se describe las características y funciones de cada uno de estos estándares.

### 5.2.1 OAUTH 2.0

Es el protocolo estándar utilizado por la industria para Autorización. Lanzado en el año 2006. Es sencillo de implementar en la capa cliente de desarrollos web, aplicaciones de escritorio, móviles y otros dispositivos.

Consiste en delegar la autenticación de usuario al servicio que gestiona las cuentas, de modo que sea éste quien otorgue el acceso para las aplicaciones de terceros. Provee flujos específicos utilizados para Autorización que han sido desarrollador por el IETF OAuth Working Group (IETF, 2012).

Para los flujos, se definen los siguientes roles:

- *Client*: Es la aplicación que quiere acceder a la cuenta de un usuario, en un servicio determinado. Para conseguirlo, debe contar con una autorización del usuario, y esta autorización se debe validar.
- *Resource Owner*: El "dueño del recurso" es el usuario que autoriza a una aplicación, para que pueda acceder a su cuenta. El acceso es limitado de acuerdo con los permisos que ha concedido el usuario en la autorización.
- *Resource Server*: Es el servidor que almacena las cuentas de usuarios
- Authorization Server: Es el servidor que verifica la identidad de los usuarios y emite los *token* de acceso a la aplicación cliente.

**Flujo o esquema:**

A continuación, se describe un flujo genérico del protocolo OAuth. El flujo se presenta en la **Ilustración 17**(Anicas, 2020)

1. La aplicación cliente solicita una autorización para acceder a los recursos de un usuario en un servicio determinado.
2. Si el usuario autoriza esta solicitud, la aplicación recibe una *authorization grant* (concesión de autorización).
3. La aplicación solicita un *access token* al *authorization server* (API) presentando su identidad y el permiso concedido anteriormente.
4. Si la identidad de la aplicación cliente se reconoce correctamente por el servicio y la concesión de autorización es válida, el *authorization server* (API) emite un *access token* a la aplicación. Con esto la autorización se ha completado.
5. La aplicación solicita un recurso al *resource server* (API) y presenta el correspondiente *access token*.
6. Si el *access token* es válido, el *resource server* (API) hace entrega del recurso a la aplicación.

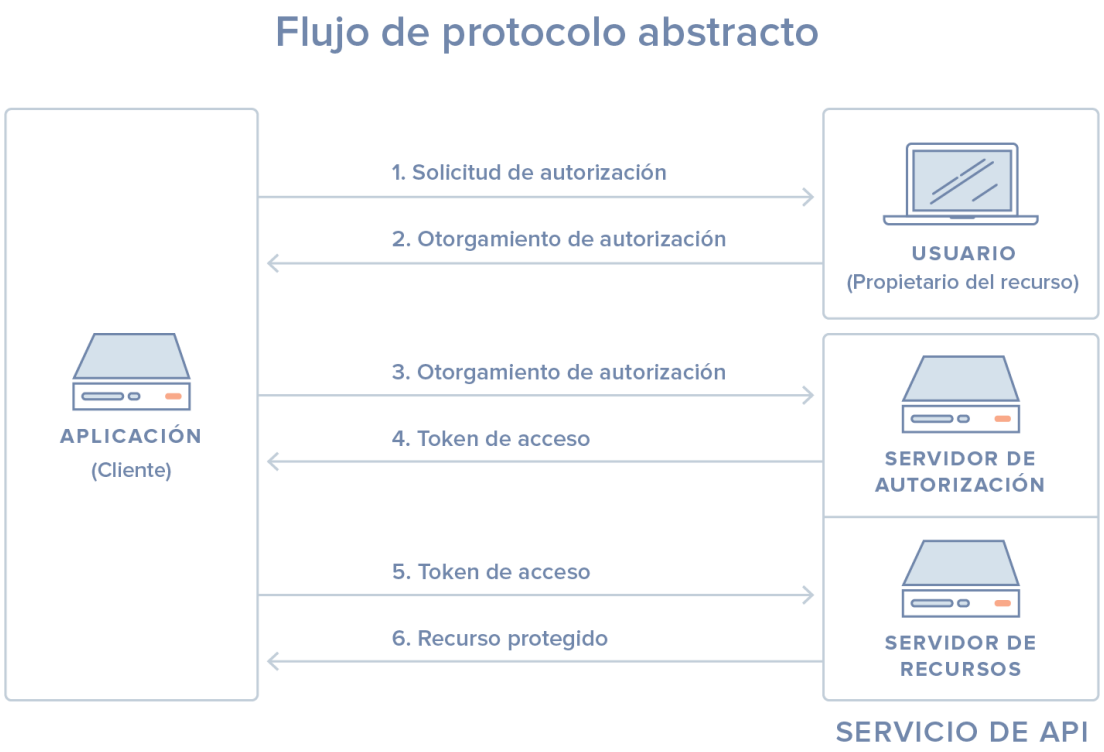



***Ilustración 17*** *Flujo genérico OAuth 2.0*[18]

**Obtención de la autorización**

En el flujo general presentado anteriormente (Ver **Ilustración 17**), los primeros cuatro pasos abarcan la obtención de una autorización y el token de acceso. El tipo de otorgamiento de la autorización depende del método utilizado por la aplicación para solicitar dicha autorización y de los tipos de autorización soportados por la API. OAuth 2 define cuatro tipos de autorización, cada uno de los cuales es útil en casos distintos:

[18] Fuente: (Anicas, 2020)

a. **Código de autorización**: usado con aplicaciones del lado del servidor

Es el más utilizado ya que ha sido optimizado para aplicaciones del lado del servidor, en donde el código fuente no está expuesto públicamente y se puede mantener la confidencialidad del cliente. Este es un flujo basado en la reorientación (*redirection*), que significa que la aplicación debe ser capaz de interactuar con el agente de usuario (i.e. el navegador web del usuario) y recibir códigos de autorización API que se enrutan a través del agente de usuario.

Flujo:

1. Se le da al usuario un enlace de código de autorización
2. El usuario autoriza a la aplicación
3. La aplicación recibe el código de autorización
4. La aplicación solicita token de acceso
5. La aplicación recibe el token de acceso
6. La aplicación puede utilizar el token para acceder a la cuenta del usuario a través de la API de servicio, limitada al alcance del acceso, hasta que el token caduque o se revoque. Si se generó un token de actualización, éste se puede usar para solicitar nuevos tokens de acceso cuando el token original ha caducado

A continuación se presenta el diagrama de este flujo en la **Ilustración 18**.


***Ilustración 18*** *Flujo de otorgamiento: Código de autorización*[19]

b. **Implícito**: utilizado con aplicaciones móviles o aplicaciones web (aplicaciones que se ejecutan en el dispositivo del usuario)

[19] Fuente: (Anicas, 2020)

El tipo de otorgamiento implícito también es un flujo basado en la reorientación, pero el token de acceso se entrega al agente-usuario para reenviarlo a la aplicación, por lo que puede estar expuesto al usuario y a otras aplicaciones en el dispositivo del usuario. El tipo de otorgamiento implícito no admite tokens de actualización.

Flujo:

1. Se le presenta al usuario un enlace de autorización que solicita un token de la APLI. Enlace de autorización implícita.
2. El usuario autoriza a la aplicación. El usuario hace clic en el enlace, primero debe iniciar sesión en el servicio para autenticar su identidad. Luego, el servicio le solicitará que autorice o deniegue el acceso de la aplicación a su cuenta.
3. El agente-usuario recibe el token de acceso con *RedirectURI*
4. El agente-usuario sigue al redirect URI pero conserva el token de acceso
5. La aplicación envía el script de extracción de tokens de acceso
6. El agente-usuario ejecuta el script proporcionado y para el token de acceso que se extrae a la aplicación
7. La aplicación está autorizada

A continuación se presenta el diagrama de este flujo en la **Ilustración 19**


***Ilustración 19*** *Flujo de otorgamiento: Implícito*[20]

c. **Credenciales de contraseña del propietario del recurso**: utilizado con aplicaciones confiables, como aquellas pertenecientes al servicio

Con este tipo de otorgamiento, el usuario proporciona sus credenciales de servicio (nombre de usuario y contraseña) directamente a la aplicación, la cual utiliza dichas credenciales para obtener del servicio un token de acceso. Este tipo de autorización solo

[20] Fuente: (Anicas, 2020)

debe habilitarse en el servidor de autorización si otros flujos no son viables. Además, solo debe utilizarse si la aplicación es confiable para el usuario.

Flujo

1. El usuario proporciona sus credenciales a la aplicación.
2. La aplicación solicitará un token de acceso desde el servidor de autorizaciones.
3. Si las credenciales del usuario son correctas, el servidor de autorización devuelve un token de acceso a la aplicación.

d. **Credenciales del cliente**: usadas con el acceso API de aplicaciones

Este tipo de otorgamiento proporciona a la aplicación una forma de acceder a su propia cuenta de servicio.

Flujo:

1. La aplicación solicita un token de acceso enviando las credenciales e ID de cliente al servidor de autorización.
2. Si se comprueban las credenciales, el servidor de autorización devuelve un token de acceso a la aplicación.
3. La aplicación está autorizada.

Ejemplo:

Si se observa un diálogo como el que se presenta en la **Ilustración 20**, se está utilizando OAuth. La aplicación está preguntando si puede acceder a los datos en su nombre.

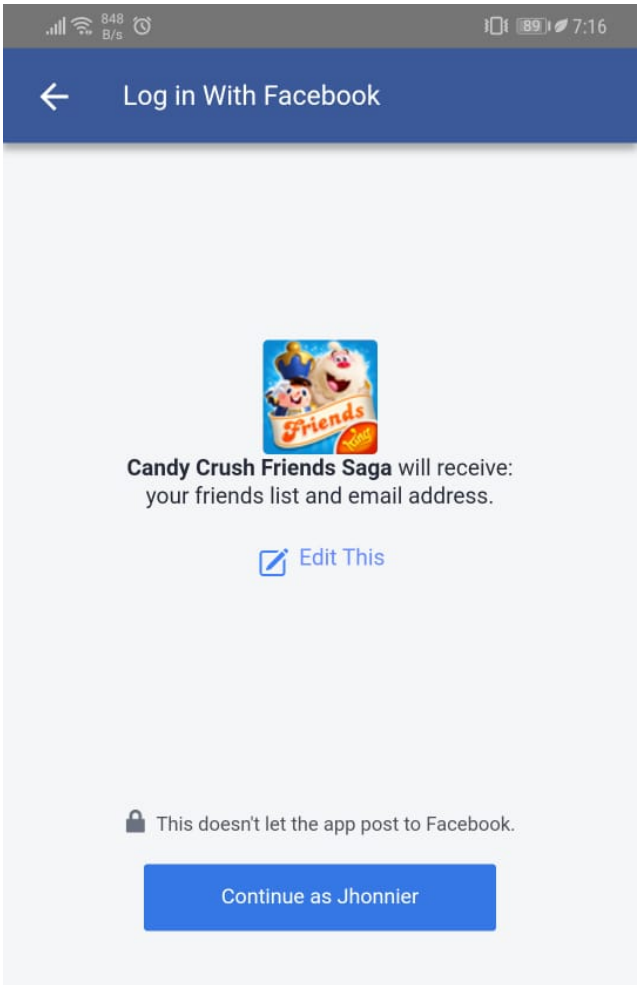



***Ilustración 20*** *Ejemplo uso OAuth*[21]

### 5.2.2 OPENID CONNECT

[21] **Fuente:** Del autor

Es un protocolo de autenticación que permite a las aplicaciones y desarrollos validar los usuarios en múltiples sitios sin la necesidad de hacerse responsable de almacenar y gestionar las contraseñas.

Es un estándar abierto patrocinado por Facebook, Microsoft, Google, PayPal, Ping Identity, Symantec y Yahoo(Foundation, 2020).

OpenID Connect 1.0 ha sido construido sobre el protocolo OAuth 2.0. Permite que el Cliente verifique la identidad del usuario final utilizando la autenticación ejecutada por un Servidor de Autorización. Adicional, permite obtener información básica del perfil del usuario final.

OpenID Connect puede ser utilizado por cliente de diferentes tipos, incluyendo aplicaciones web, móviles, Javascript.
La especificación final fue lanzada el 26 de febrero de 2014.

OpenID Connect es la tercera generación de la tecnología OpenID. El OpenID original fue una herramienta que nunca tuvo reconocimiento comercial, pero logró que la industria visionara lo que se podría lograr con ella. Su sucesor, OpenID 2.0, estuvo mejor diseñado y ofrecía una excelente seguridad. Sin embargo, sus dos mayores limitantes eran que sólo aplicaba para aplicaciones web y al estar diseñado sobre XML provocaba algunos problemas de implementación.

Así nace OpenID Connect con el objetivo de ser fácilmente implementado y operar sobre entornos de producción a gran escala. Se basa en mensajes JSON sobre HTTP permitiendo que un programador con la suficiente experiencia pueda implementarlo desde cero utilizando librerías estándar para verificación de firmas.

Se definen tres roles:

- Usuario final o entidad que solicita verificar su identidad.
- Entidad que busca verificar la identidad del usuario final. RP por sus siglas en inglés: Relying Party.
- Proveedor OpenID (OP) quien registra la URL OpenID y puede verificar la identidad del usuario final.

**Flujo o esquema:**

1. El RP inicia la autenticación del usuario redireccionando al OP. La solicitud de autenticación es básicamente una solicitud de autorización OAuth 2.0 para acceder a la identidad del usuario.
2. En el OP, el usuario será autenticado, verificando si existe una sesión válida y si no ésta no existe, solicitará credenciales al usuario y luego se le preguntará si está de acepta loguearse en el RP.
3. El OP redireccionará con un código de autorización si el acceso es exitoso o un código de error si el acceso fue denegado.
4. El RP debe validar el parámetro *state* y usar el código *code* para intercambiar información del Token.

5. El código de autorización es una credencial intermedia que codifica la autorización obtenida en el paso 1; por lo tanto, sólo es útil al servidor OP. Para obtener el ID Token, el RP debe enviar este código de autorización al OP pero esta vez con una solicitud directa. Debe hacerse de esta forma por dos razones:
    - Para autenticar los clientes con el OP antes de revelar los tokens.
    - Para entregar los tokens directamente al RP evitando exponerlos en el navegador

    La identificación del cliente y sus credenciales son enviados en el encabezado de la Autorización o utilizando JWT evitando exponer las credenciales, tiene tiempo de expiración y provee mayor seguridad.
6. En caso de éxito, el servidor OP retornará un objeto JSON con el ID Token y un token de acceso. Estos datos deben ser validados por el RP antes de que puedan ser aceptados.

Se presenta el flujo anterior en la **Ilustración 21**.

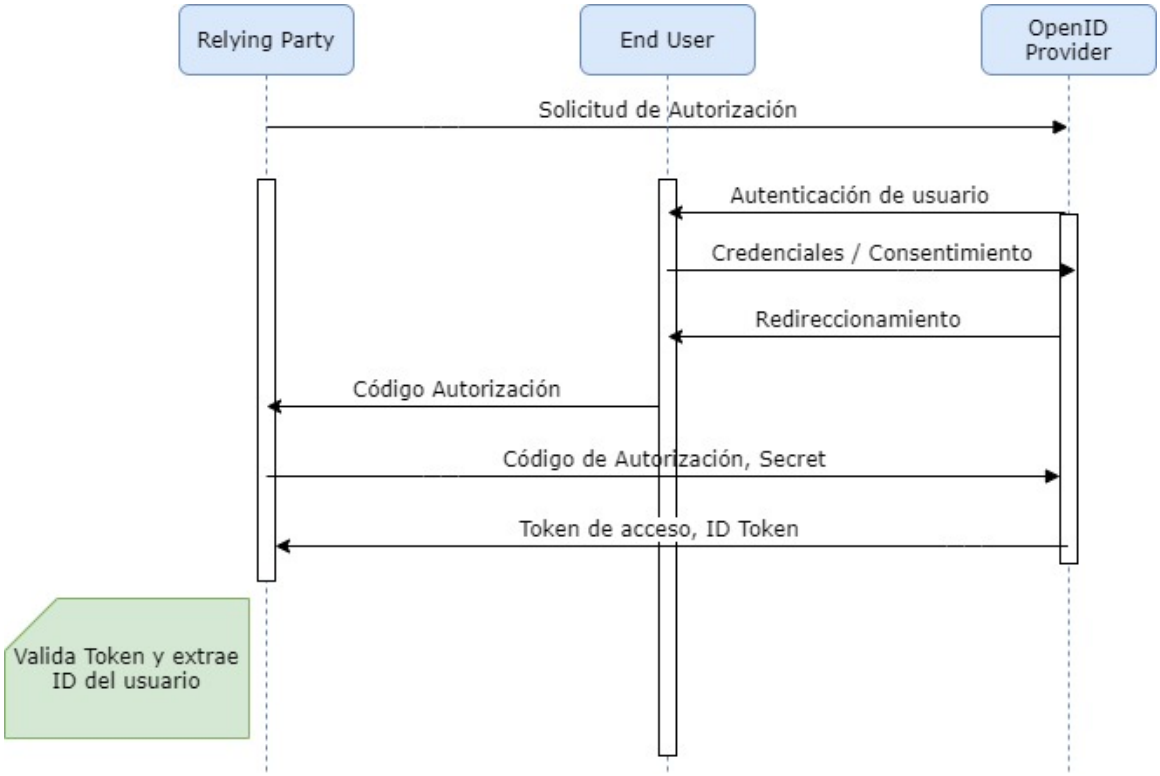



***Ilustración 21*** *Flujo OpenID Connect*[22]

### 5.2.3 SAML

SAML es el acrónimo de "Security Assertion Markup Language", el cual es un estándar de código abierto basado en XML que permite el intercambio de autenticación y autorización de datos entre distintas partes. Su primera especificación fue creada en el año 2001 por **Organization for the Advancement of Structured Information Standards** (**OASIS**) (OASIS, 2020). En el año 2005 fue ratificada SAML 2.0, la cual sigue vigente hasta ahora.

---

[22] **Fuente:** Del autor

- SAML 1.0: 2002
- SAML 1.1: 2003
- SAML 2.0: 2005
- SAML 2.1: actualmente en desarrollo.

El estándar SAML está formado por varios componentes que aportan **todas las funciones necesarias** para **definir y transmitir información de forma segura.**

SAML permite comunicar identidades entre organizaciones, en otras palabras permite manejar SSO a través de internet o redes académicas para nuestro interés particular. Este elimina la necesidad de mantener credenciales como contraseñas en múltiples ubicaciones lo cual es muy importante por las siguientes razones:

- Mejora la seguridad al eliminar credenciales almacenadas en diferentes lugares, lo que disminuye la posibilidad de que alguno de estos repositorios con contraseñas sean vulnerados y los datos comprometidos.
- Facilita el acceso de los usuarios a las aplicaciones dado que con el mismo nombre de usuario y clave pueden acceder a estas. Adicional con un único inicio de sesión podrán tener acceso a diferentes aplicaciones.
- Disminuye tiempo y costo en la gestión de los usuarios en las organizaciones.

A continuación se revisa su funcionamiento, SAML tiene 3 componentes principales:

- Usuarios que requieren acceder a las aplicaciones.


***Ilustración 22*** *Representación Usuario*[23]

- Proveedor de identidad (IdP).


***Ilustración 23*** *Representación IdP*[24]

- Aplicaciones o servicios, los cuales se conocerán como proveedores de servicios (SP).


***Ilustración 24*** *Representación SP*[25]

Para la implementación de SAML, es necesario instalar una solución de federación de identidad utilizando los 3 componentes mencionados.

[23] Fuente: Del autor
[24] Fuente: Del autor
[25] Fuente: Del autor

Las soluciones más conocidas que cumplen con el estándar SAML se presentan la **Ilustración 25**:


***Ilustración 25*** *Soluciones conocidas que cumplen estándar SAML*[26]

Las credenciales de los usuarios son accedidas a través del IdP a un directorio de usuarios. Los más usados son OpenLdap o Directorio Activo de Microsoft. Estos son gestionados por la organización a la cual pertenecen los usuarios.

A continuación, la **Ilustración 26** describe el funcionamiento general de SAML: Cuando el usuario quiere ingresar a un recurso o servicio web, lo hace a través de un navegador al SP. El SP puede estar realmente en cualquier parte, ya sea en la intranet o en algún lugar del mundo en una solución de nube pública por ejemplo. Una vez el usuario ingresa sus credenciales, la solución de federación de identidad instalada, las verifica en el IdP. Si la validación es exitosa, este construye un mensaje con información del usuario y es entregado al software de federación de identidad en el SP. Allí valida si el mensaje

[26] Fuente: ("miniOrange Secure It Right : Identity and Access Management Solution," 2020)

proviene de un IdP conocido, y si es así, crea una sesión para el usuario validado y le permite el acceso a la aplicación o servicio que el usuario requiere.

En la **Ilustración 27** se presenta el flujo de SAML.

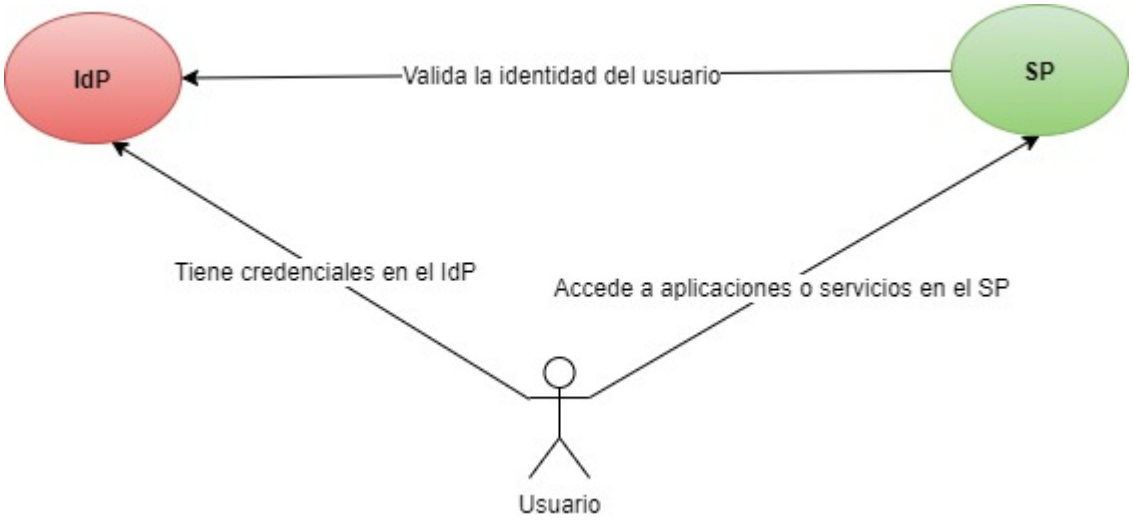



***Ilustración 26*** *Funcionamiento general SAML*[27]

[27] **Fuente:** Del autor

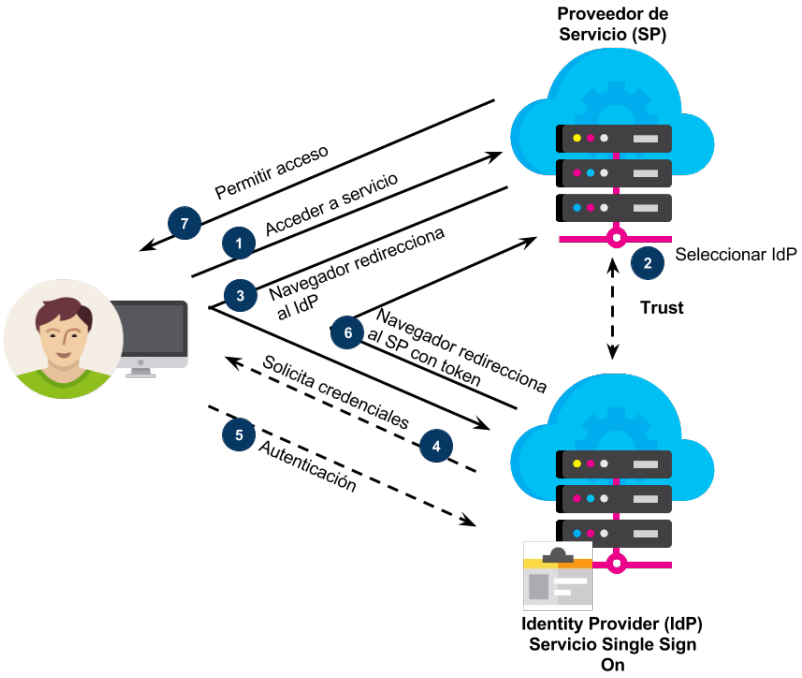



***Ilustración 27*** *Flujo general SAML*[28]

El proceso anterior, es completamente transparente para el usuario. Desde el punto de vista de este, solo hizo clic e ingresó sus credenciales. El procedimiento SAML SSO, que permite al usuario utilizar varias aplicaciones con un único inicio de sesión, se utiliza más allá de los procesos y aplicaciones internas de las empresas: actualmente el inicio de sesión único está consolidado en los servicios que ofrecen muchas aplicaciones web, especialmente dentro de los sectores de la banca online y de las aplicaciones móviles. A veces, el usuario ni siquiera se da cuenta de que ha pasado de una aplicación a otra mediante este tipo de servicios. Por ejemplo, un cliente inicia sesión en la página web de su banco y es probable que acceda a otros sistemas backend sin darse cuenta. Esto ocurre, por ejemplo,

[28] Fuente: (UY, 2020)

si abre una cuenta de ahorro, un depósito o una cuenta de tarjeta de crédito. Gracias a SAML, el usuario piensa que todas esas acciones han tenido lugar en un mismo programa.

El esquema anterior es una implementación básica. Uno de los beneficios de SAML es se puede implementar a múltiples SP y con varios IdP, y es el esquema que se utiliza en Federación de Identidad, tal como se presenta en la **Ilustración 28**

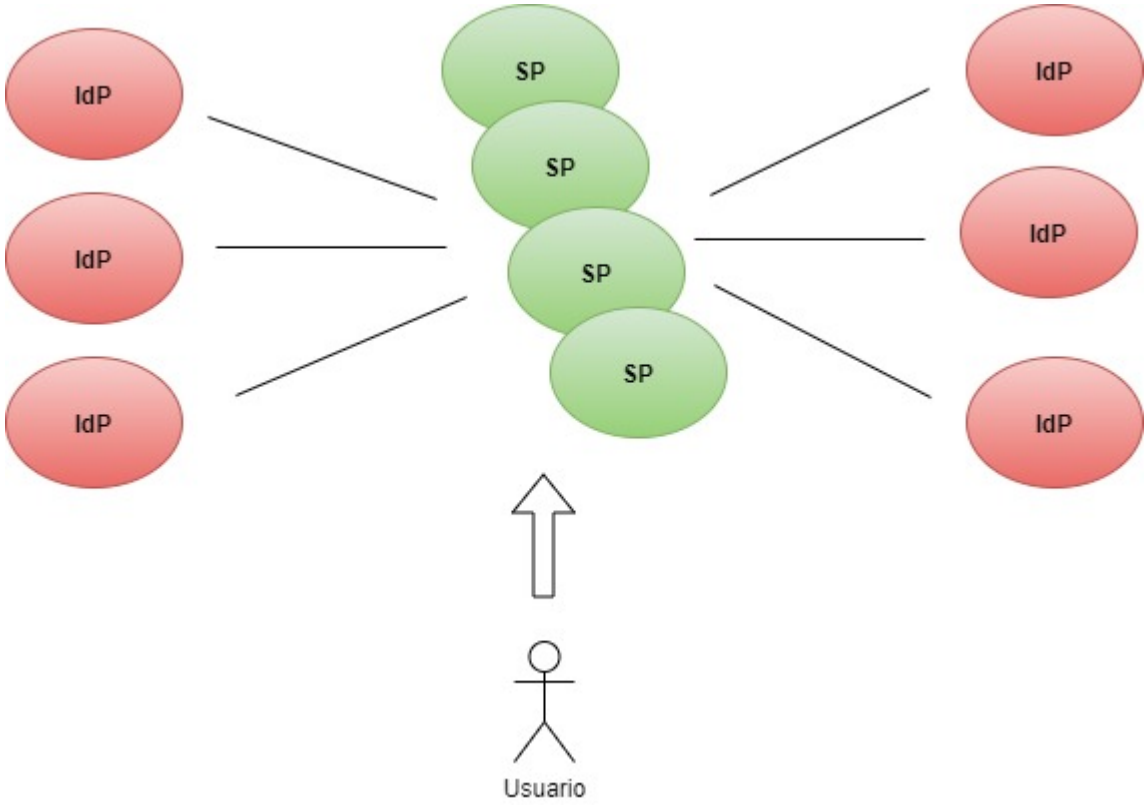



***Ilustración 28*** *Representación SAML multiples SP y varios IdP*[29]

**Funciones de cada componente de SAML**

[29] **Fuente:** Del autor

**Aserciones**

Una aserción o assertion SAML puede incluir una o más declaraciones o statements sobre las propiedades (identidad, atributos) y los permisos de un usuario. El responsable de crearla es el IdP correspondiente, es decir, la base de datos que corresponda al usuario, que utiliza XML como lenguaje de marcado. Cada aserción recibe una firma digital, que primero tiene que ser comprobada y verificada por el service provider al que se desea acceder, es decir, por la aplicación pertinente. De esta forma, es posible garantizar la integridad y autenticidad de la aserción, que recibe el nombre, una vez firmada, de token SAML. Después de realizar la verificación, el proveedor de servicios analiza el contenido concreto y luego decide si otorga o no acceso al usuario y en caso afirmativo, qué tipo de acceso otorga.

El estándar SAML 2.0 especifica los tres tipos siguientes de declaraciones en la aserción:

- *Authentication Statements*: son expedidas por la entidad que ha llevado a cabo el proceso de autentificación del usuario. En una declaración de este tipo se recoge quién la ha emitido, el sujeto autentificado, el período de validez y otros datos relacionados con la autentificación.
- *Attribute Statements*: contienen detalles específicos sobre el usuario y pueden ser comunicadas a la aplicación mediante el token SAML correspondiente.

- *Authorization* Decision Statements: recogen datos sobre lo que le está o no permitido hacer al usuario. Por ejemplo, si está o no autorizado a acceder a un determinado recurso.

**Protocolos**

La especificación SAML 2.0 establece una serie de protocolos de solicitud o respuesta con los que la aplicación puede, por ejemplo, solicitar una aserción o pedir a un usuario que se autentique. Se utilizan los siguientes protocolos:

- *Authentication Request Protocol*: define mensajes del tipo <AuthnRequest>, que son necesarios para consultar aserciones con Authentication Statements de un usuario seleccionado. Generalmente, es un proveedor de servicios el que emite la solicitud y suele utilizar un perfil SAML 2.0 navegador Web SSO y contestada por un proveedor de identidad tras haber completado con éxito un proceso de autentificación del usuario.
- *Assertion Query y Request Protocol*: es necesario para solicitudes con las que, en general, se pueden obtener aserciones SAML ya existentes. Es posible solicitar una aserción siguiendo distintos parámetros como, por ejemplo, que contenga unas declaraciones determinadas.
- *Single Logout Protocol*: define solicitudes que inician el cierre casi simultáneo de todas las sesiones abiertas pertenecientes a un mismo usuario. Este tipo de mensajes

pueden enviarse directamente tanto al usuario como a un proveedor de identidad o de servicio. Este último suele considerarse cuando la sesión de un usuario ha expirado.

- *Artifact Resolution Protocol*: se utiliza para transportar los mensajes SAML por separado a través de un canal seguro o en un tamaño reducido para ahorrar recursos. Permite el envío de referencias y aserciones que también se denominan "artifact" y son considerablemente más pequeñas que el propio mensaje. El protocolo también permite borrar estas referencias para recibir el mensaje original.
- *Name Identifier Management Protocol*: este protocolo proporciona mecanismos para modificar el valor o el formato del nombre de un usuario. La solicitud puede proceder de un proveedor de servicio o de un proveedor de identidad. Además, este protocolo también puede utilizarse para eliminar aquellos enlaces entre proveedores de servicio y proveedores de identidad que fueron creados para autenticar la identidad del usuario original.
- *Name Identifier Mapping Protocol*: este protocolo define mensajes de solicitud y de respuesta para que dos proveedores de servicio puedan comunicarse. Basándose en este tipo de mensaje, una aplicación puede solicitar un identificador para un usuario al proveedor de identidad con el fin de acceder a otra aplicación.

**Bindings**

Las especificaciones para “mapear” un protocolo SAML sobre un determinado protocolo de transporte reciben el nombre de binding. Se definen varios tipos, entre los que se encuentran, por ejemplo, el *SOAP Binding*, que sirve para definir cómo los mensajes del protocolo SAML se intercambian, integrados en mensajes de SOAP, y especifica cómo dichos mensajes SOAP se transportan sobre HTTP. Por su parte, el *HTTP Redirect Binding* define cómo se pueden transportar mensajes del protocolo SAML a través del procedimiento de redirección HTTP. Se pueden citar como ejemplo de otros tipos de bindings en el estándar SAML 2.0:

*Reverse SOAP Binding*

*HTTP POST Binding*

*HTTP Artifact Binding*

*SAML URI Binding*

**Perfiles**

SAML es un estándar general y se caracteriza por su flexibilidad, lo que le permite poder ser utilizado como marco en muchos supuestos diferentes. Sin embargo, para que ciertas aplicaciones puedan ser compatibles con SAML, a veces es necesario restringir esa flexibilidad. Un perfil o profile se utiliza para combinar determinadas aserciones, protocolos y bindings para componer en la práctica un supuesto de uso concreto de la especificación SAML. Uno de los perfiles más utilizados es Web Browser SSO Profile,

que especifica el marco para poner en marcha la autentificación única SSO en SAML. Incluye todos los componentes necesarios para definir la comunicación de las garantías de autentificación SAML entre el proveedor de identidad y el proveedor de servicios, que son necesarias para la autentificación única en un navegador web. El estándar también define los siguientes perfiles adicionales:

*Enhanced Client and Proxy (ECP) Profile*

*Identity Provider Discovery Profile*

*Single Logout Profile*

*Name Identifier Management Profile*

*Artifact Resolution Profile*

*Assertion Query/Request Profile*

*Name Identifier Mapping Profile*

### 5.2.4 Comparativo OAUTH 2.0 vs. OPENID CONNECT vs. SAML

En la **Tabla 14** se presenta el comparativo para los tres estándares vistos:

| | **OAuth 2.0** | **OpenID Connect** | **SAML** |
|---|---|---|---|
| **Tipo de estándar** | Estándar abierto | Estándar abierto | Estándar abierto |
| **Historia** | Desarrollado por Twitter y Google en 2006 | Desarrollado por OpenID Foundation en 2014 | Desarrollado por OASIS en 2001 |
| **Funcionalidad** | Autorización | Autenticación | Autenticación y Autorización |
| **Uso principal** | API de autorización | SSO para consumidores | SSO en entornos empresariales y redes académicas como eduGAIN. |
| **Clientes soportados** | Aplicaciones web, aplicaciones de escritorio, móviles y otros dispositivos | Aplicaciones web, móviles, Javascript | Aplicaciones web |
| **Formato** | JSON | JSON | XML |

***Tabla 14*** *Comparativo OAuth – OpenID Connect - SAML*

### 5.2.5 Selección de estándar

Para las tecnologías estudiadas y con el propósito de realizar una selección objetiva de la tecnología a utilizar, se toma como base el área de proceso "Análisis de Decisiones y Resolución" (DAR) del "Capability Maturity Model" (CMMi)(SEI Administrative Agent, 2010).

Se define como estrategia para la selección del estándar la definición de 5 criterios otorgando a cada uno de ellos un peso de acuerdo con su importancia en la implementación de la arquitectura para dar solución a las necesidades relacionadas con federación de identidad en la Universidad Tecnológica de Pereira.

Los criterios y los pesos fueron seleccionados utilizando juicio de expertos entre integrantes de la Maestría en Ingeniería de Sistemas y el área de Administración de Redes y Seguridad de la Información (UTP).

A continuación, se definen los criterios.

a. Estándar abierto (15%): Hace referencia a la importancia de poder utilizar herramientas libres en la implementación de la arquitectura.
b. Funcionalidades (20%): Se toma en cuenta si se incluyen funcionalidades de Autenticación, Autorización o ambas.

c. Entornos de Aplicación (30%): Es importante elegir un estándar que sea ampliamente utilizado en el ámbito académico y empresarial. Tendrá mayor puntuación el estándar que esté ampliamente difundido e implementado en una red académica de interfederación tipo eduGAIN. Este criterio es de especial relevancia dado que el actual proyecto de investigación tiene aplicación en instituciones académicas.
d. Madurez (20%): Hace referencia al tiempo que lleva el estándar en el mercado. Es importante por la cantidad de implementaciones que pueda tener.
e. Formato (15%): Extensibilidad, seguridad, usabilidad, consumo de recursos.

Cada criterio tendrá una puntuación de 1 ó 2, siendo:

a. Estándar abierto:
    - 1: Estándar propietario
    - 2: Estándar abierto
b. Funcionalidades:
    - 1: Sólo una de las funcionales: autenticación o autorización
    - 2: Cumple las dos funcionalidades: autenticación y autorización
c. Entornos de Aplicación:
    - 1: Si el estándar es utilizado es entornos empresariales o comerciales

- 2: Si el estándar es utilizado en entornos académicos. Este criterio tiene mayor importancia para el proyecto al tratarse de una implementación en instituciones académicas.

d. Madurez:

- 1: Si el estándar tiene menos de 10 años en el mercado.
- 2: Si el estándar tiene más de 10 años en el mercado.

e. Formato :

- 1: Si el estándar soporta formato diferente a XML.
- 2: Si el estándar soporta XML.

De acuerdo con el procedimiento anterior, se presenta a continuación la calificación de los estándares en **Tabla 15**

| CRITERIO | PESO | OAuth 2.0 | OpenID Connect | SAML |
|---|---|---|---|---|
| **Estándar abierto** | **15%** | 2 | 2 | 2 |
| **Funcionalidades** | **20%** | 1 | 1 | 2 |
| **Entornos de aplicación** | **30%** | 1 | 1 | 2 |
| **Madurez** | **20%** | 2 | 1 | 2 |
| **Formato** | **15%** | 1 | 1 | 2 |
| | **100%** | **1,35** | **1,15** | **2** |

***Tabla 15*** *Tabla de decisión de estándar*

El estándar con mayor puntaje es SAML debido a que es un estándar de código abierto, que ofrece capacidades tanto de Autenticación como de Autorización, es

ampliamente utilizado en entornos empresariales y académicos destacando la red edugain y soluciones como Directorio Activo de Microsoft. Es el más antiguo de los tres presentados.

## 5.3 ESQUEMA ARQUITECTÓNICO PARA LA FEDERACIÓN DE IDENTIDAD

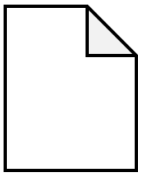
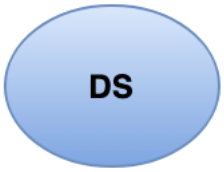
Esta etapa del proyecto corresponde a la arquitectura propuesta para la implementación de federación de identidad en la UTP, utilizando el estándar SAML 2.0.

Se mostrarán los elementos utilizados, escenarios que hacen parte de la arquitectura, el diagrama general de la arquitectura y el modelado de la solución.

### 5.3.1 Elementos

En primera instancia se definen los elementos a utilizar en la arquitectura basados en los requerimientos de SAML 2.0

| Elementos | DESCRIPCIÓN |
|---|---|
|  | Proveedor de servicios (SP): Este elemento es el que federa los servicios. |

| | |
|---|---|
|  | Proveedor de Identidad (IdP): Este elemento es el encargado de autenticar al usuario final contra una base de datos usando el protocolo LDAP. |
|  | Base de datos de usuarios: Repositorio de usuarios con soporte para el protocolo LDAP. |
|  | Metadata: Datos que se intercambian entre el IdP y SP. |
|  | Aserciones de SAML: Paquete de información suministrada por el IdP o el SP. |
|  | Servicio de Descubrimiento (DS): Este elemento es el que permite la interefederación. Este tiene un listado de los IdPs que se pueden utilizar para autenticar usuarios que pertenecena organizaciones diferentes. |
|  | Entidad donde se implementa el escenario. |

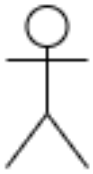
| | |
|---|---|
|  | Usuario. |

***Tabla 16*** *Elementos de la arquitectura*

### 5.3.2 Escenarios/Estados

Se plantean 3 posibles escenarios o estados que pueden darse en alguna institución de acuerdo con su infraestructura y recursos disponibles.

#### *5.3.2.1 Escenario/estado fase 1 de instanciación de la federación de identidad.*

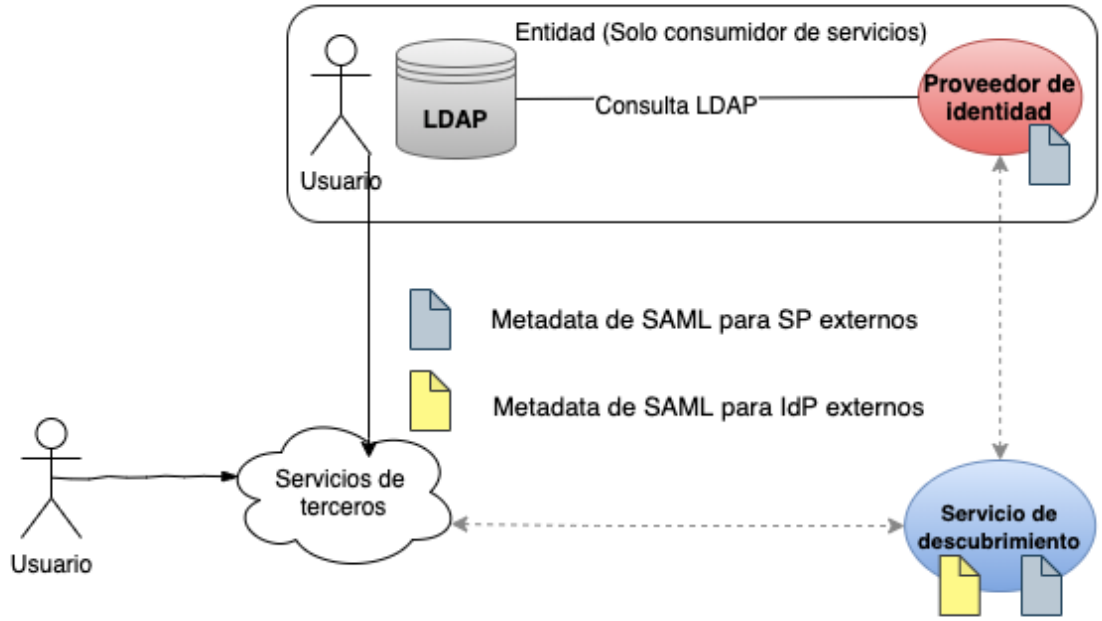



***Ilustración 29*** *Escenario 1*[30]

[30] **Fuente:** Del autor

En este escenario, la organización cuenta con un IdP que tiene acceso al directorio de usuarios de la organización. Este IdP es accedido a través del servicio de descubrimiento cuando los usuarios de la institución tratan de acceder a un servicio alojado en otra institución. (Ver **Ilustración 29**)

#### *5.3.2.2 Escenario/estado fase 2 de instanciación de la federación de identidad.*

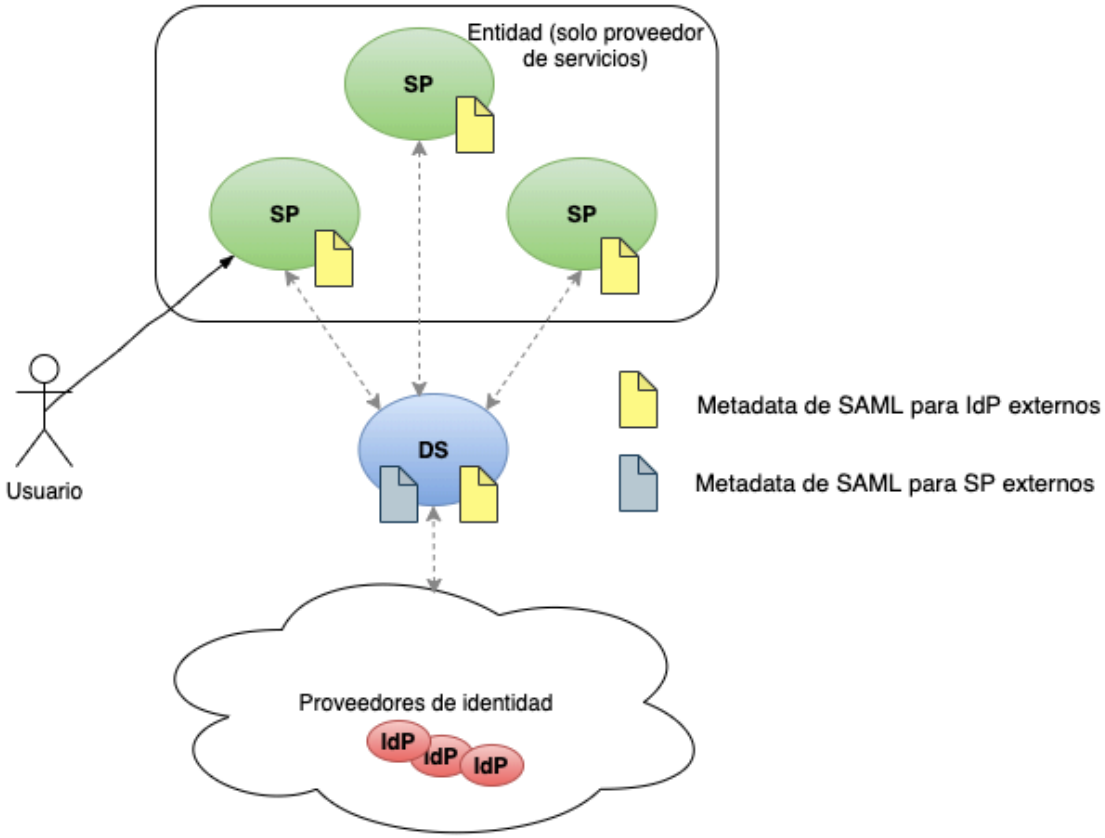



***Ilustración 30*** *Escenario 2*[31]

En este caso la organización cuenta con servicios que se ofrecen para ser accedidos por usuarios de otras instituciones a través del servicio de descubrimiento. (Ver **Ilustración 30**)

[31] **Fuente:** Del autor

### *5.3.2.3 Escenario/estado fase 3 de instanciación de la federación de identidad.*

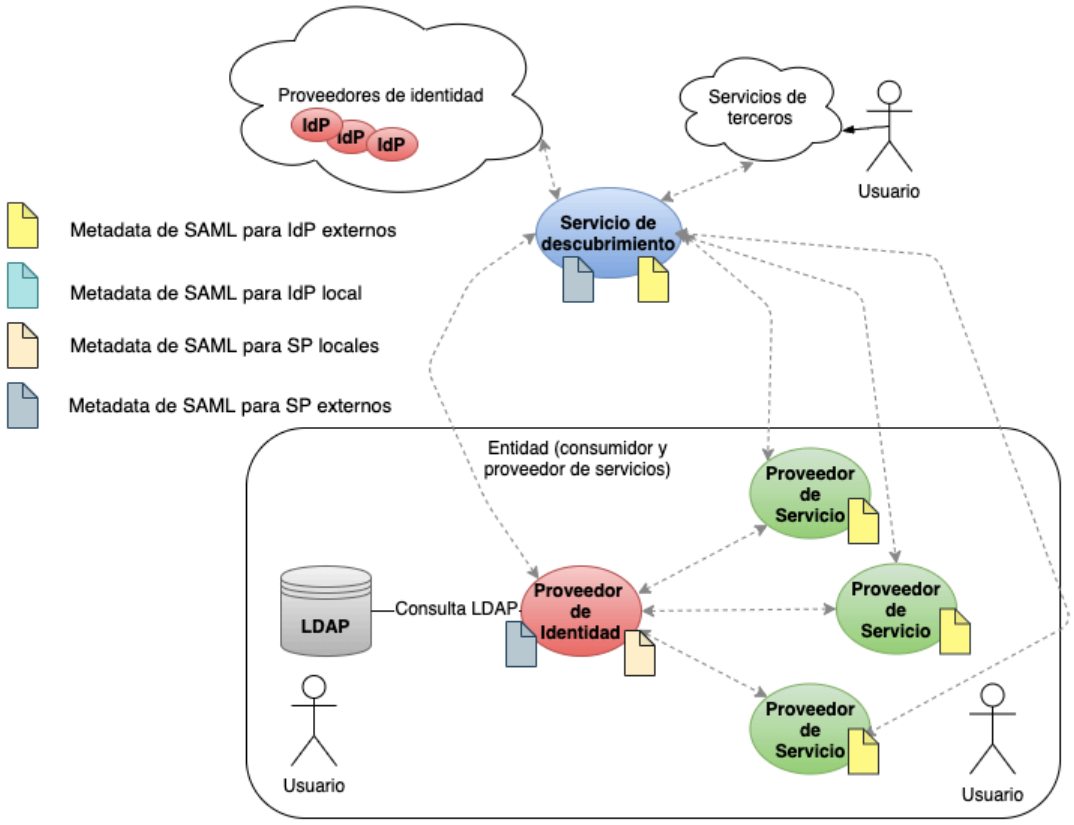



***Ilustración 31*** *Escenario 3*[32]

Este escenario es el más completo y en este la institución cuenta con un IdP, directorio de usuarios y varios servicios federados. Los servicios federados pueden ser accedidos por los usuarios de la institución, o por usuarios de otras instituciones a través del servicio de descubrimiento. Por otro lado, los usuarios de la institución tienen la posibilidad de acceder a servicios de otras instituciones utilizando el DS. (Ver **Ilustración 31**)

---

[32] **Fuente:** Del autor

### *5.3.2.4 Arquitectura con todos los escenarios/estados*

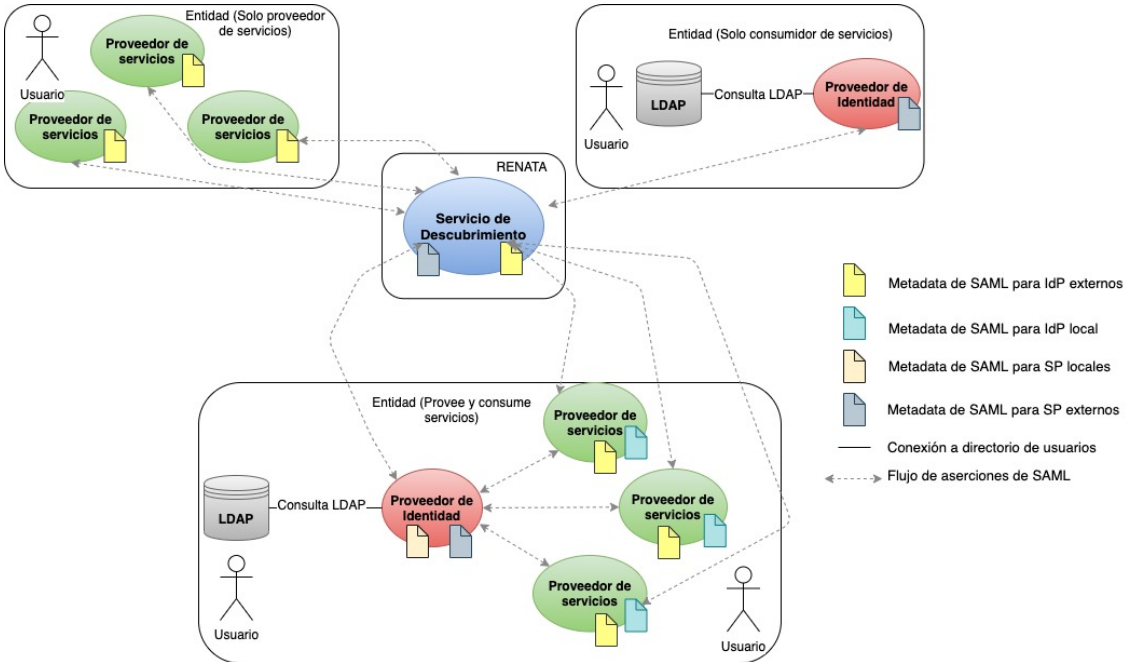



***Ilustración 32*** *Arquitectura propuesta*[33]

La arquitectura propuesta contempla los tres escenarios presentados anteriormente, tal como se identifica en la **Ilustración 32.** El servicio de descubrimiento (*Discovery Service*) posibilita la interfederación de identidad.

[33] **Fuente:** Del autor

### 5.3.3 Modelo de la arquitectura de federación de identidad con bpmn

Con el propósito de facilitar la comprensión de la arquitectura propuesta, se realiza un esquema con la notación para el modelado de procesos de negocio (BPMN). La **Ilustración 33** evidencia la forma como interactúan los componentes de la arquitectura y sus respectivas actividades.

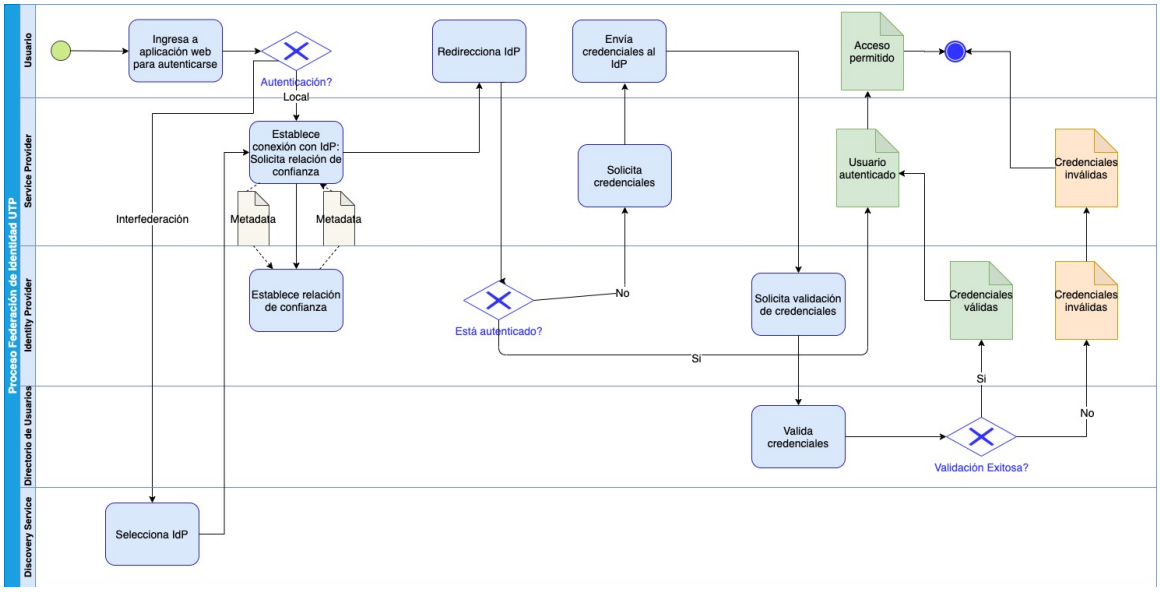



***Ilustración 33*** *Diagrama BPMN de la arquitectura propuesta*[34]

Tomando como referencia la **Ilustración 33** la cual cuenta con proveedor de identidad, directorio de usuarios, proveedor de servicios y servicio de descubrimiento, se describen las posibles acciones que se pueden desarrollar.

[34] **Fuente:** Del autor

#### *5.3.3.1 Caso: autenticación en el IdP local y el usuario ya se había autenticado.*

| PASO | ACTOR | ACCIÓN |
|---|---|---|
| 1 | Usuario/Navegador | Ingresa a aplicación web para registrarse en IdP local |
| 2 | SP | Establece relación de confianza con el IdP. Esto requiere que el IdP tenga registrada la metadata del SP y viceversa |
| 3 | Usuario/Navegador | Es redireccionado al IdP para que ingrese sus credenciales |
| 4 | IdP | Si el usuario ya está autenticado, envía mensaje al SP notificándolo |
| 5 | SP | Concede el acceso a la aplición web |

***Tabla 17*** *Caso: autenticación en el IdP local y el usuario ya se había autenticado*

#### *5.3.3.2 Caso: autenticación en el IdP local, el usuario no se había autenticado previamente y la autenticación es exitosa.*

| PASO | ACTOR | ACCIÓN |
|---|---|---|
| 1 | Usuario/Navegador | Ingresa a aplicación web para registrarse en IdP local |
| 2 | SP | Establece relación de confianza con el IdP. Esto requiere que el IdP tenga registrada la metadata del SP y viceversa |
| 3 | Usuario/Navegador | Es redireccionado al IdP para que ingrese sus credenciales |
| 4 | IdP | Solicita credenciales del usuario |
| 5 | Usuario/Navegador | Envía credenciales al IdP |

| | | |
|---|---|---|
| 6 | IdP | Solicita validación de credenciales al Directorio de usuarios |
| 7 | Directorio de usuarios | Si validación de credenciales es exitosa, notifica al IdP |
| 8 | IdP | Notifica al SP el usuario autenticado |
| 9 | SP | Concede el acceso a la aplición web |

***Tabla 18*** *Caso: autenticación en el IdP local, el usuario no se había autenticado previamente y la autenticación es exitosa*

#### *5.3.3.3 Caso: autenticación en el IdP local, el usuario no se había autenticado previamente, y la autenticación no es exitosa.*

| PASO | ACTOR | ACCIÓN |
|---|---|---|
| 1 | Usuario/Navegador | Ingresa a aplicación web para registrarse en IdP local |
| 2 | SP | Establece relación de confianza con el IdP. Esto requiere que el IdP tenga registrada la metadata del SP y viceversa |
| 3 | Usuario/Navegador | Es redireccionado al IdP para que ingrese sus credenciales |
| 4 | IdP | Solicita credenciales del usuario |
| 5 | Usuario/Navegador | Envía credenciales al IdP |
| 6 | IdP | Solicita validación de credenciales al Directorio de usuarios |

| | | |
|---|---|---|
| 7 | Directorio de usuarios | Si validación de credenciales no es exitosa, notifica al IdP |
| 8 | IdP | Notifica al SP el usuario no autenticado |
| 9 | SP | No concede el acceso a la aplición web |

***Tabla 19*** *Caso: autenticación en el IdP local, el usuario no se había autenticado previamente, y la autenticación no es exitosa*

#### *5.3.3.4 Caso: autenticación en el IdP externo y el usuario ya se había autenticado.*

| PASO | ACTOR | ACCIÓN |
|---|---|---|
| 1 | Usuario/Navegador | Ingresa a aplicación web para seleccionar IdP externo para autenticarse |
| 2 | DS | Selecciona IdP y se lo notifica al SP |
| 3 | SP | Establece relación de confianza con el IdP. Esto requiere que el IdP tenga registrada la metadata del SP y viceversa |
| 4 | Usuario/Navegador | Es redireccionado al IdP para que ingrese sus credenciales |
| 5 | IdP | Si el usuario ya está autenticado, envía mensaje al SP notificándolo |
| 6 | SP | Concede el acceso a la aplición web |

***Tabla 20*** *Caso: autenticación en el IdP externo y el usuario ya se había autenticado*

#### *5.3.3.5 Caso: autenticación en el IdP externo, el usuario no se había autenticado previamente y la autenticación es exitosa.*

| PASO | ACTOR | ACCIÓN |
|---|---|---|
| 1 | Usuario/Navegador | Ingresa a aplicación web para seleccionar IdP externo para autenticarse. |
| 2 | DS | Selecciona IdP y se lo notifica al SP |
| 3 | SP | Establece relación de confianza con el IdP. Esto requiere que el IdP tenga registrada la metadata del SP y viceversa |
| 4 | Usuario/Navegador | Es redireccionado al IdP para que ingrese sus credenciales |
| 5 | IdP | Solicita credenciales del usuario |
| 6 | Usuario/Navegador | Envía credenciales al IdP |
| 7 | IdP | Solicita validación de credenciales al Directorio de usuarios |
| 8 | Directorio de usuarios | Si validación de credenciales es exitosa, notifica al IdP |
| 9 | IdP | Notifica al SP el usuario autenticado |
| 10 | SP | Concede el acceso a la aplición web |

***Tabla 21*** *Caso: autenticación en el IdP externo, el usuario no se había autenticado previamente y la autenticación es exitosa*

#### *5.3.3.6 Caso: autenticación en el IdP externo, el usuario no se había autenticado previamente y la autenticación no es exitosa.*

| PASO | ACTOR | ACCIÓN |
|---|---|---|
| 1 | Usuario/Navegador | Ingresa a aplicación web para seleccionar IdP externo para autenticarse |
| 2 | DS | Selecciona IdP y se lo notifica al SP |
| 3 | SP | Establece relación de confianza con el IdP. Esto requiere que el IdP tenga registrada la metadata del SP y viceversa |
| 4 | Usuario/Navegador | Es redireccionado al IdP para que ingrese sus credenciales |
| 5 | IdP | Solicita credenciales del usuario |
| 6 | Usuario/Navegador | Envía credenciales al IdP |
| 7 | IdP | Solicita validación de credenciales al Directorio de usuarios |
| 8 | Directorio de usuarios | Si validación de credenciales no es exitosa, notifica al IdP |
| 9 | IdP | Notifica al SP el usuario no autenticado |
| 10 | SP | No concede el acceso a la aplición web |

***Tabla 22*** *Caso: autenticación en el IdP externo, el usuario no se había autenticado previamente y la autenticación no es exitosa*

### *5.3.3.7 Justificación de la arquitectura propuesta*

La arquitectura propuesta está basada en el estándar SAML. Este estándar esta basado en un framework de XML que permite el intercambio seguro de información entre componentes de su arquitectura, soporta autenticación y autorización, federación de identidad e interfederación.

Los escenarios propuestos permiten seleccionar el que mas se ajuste a las necesidades de la Universidad, facilitando su implementación de acuerdo con la madurez que alcance la institución con la federación de identidad.

- **Aporte de la arquitectura propuesta a los problemas y necesidades identificadas en el punto 5.1.1.**

  Facilita el aprovechamiento de los recursos existentes a través de la federación de servicios.

  Brinda un mecanismo para acceder a recursos de grupos de investigación permitiendo compartirlos, logrando un mejor aprovechamiento de estos.

  Le permite a la institución orientar la adquisión de nuevos recursos computacionales.

  Se tiene visibilidad de las capacidades de los grupos de investigación al interior y exterior de la UTP.

- **Aporte de la arquitectura propuesta a las oportunidades identificadas en el punto 5.1.2**

  En los grupos de investigación se han identificado 137 recursos computacionales candidatos a ser federados con la arquitectura propuesta.

  La federación de identidad facilita el acceso de estos recursos a la población académica de otras instituciones.

  Facilita el acceso a recursos de otras instituciones a nuestra población académica.

## 5.4 PROTOTIPO FUNCIONAL DE FEDERACIÓN DE IDENTIDAD

En esta sección se muestra el diagrama del piloto funcional basado en la arquitectura propuesta, las herramientas que se utilizaron, el proceso de instalación y configuración de dichas herramientas y el diagrama de red final.

### 5.4.1 Diseño del prototipo funcional

En la **Ilustración 34** se presenta el diagrama de despligue del prototipo funcional.

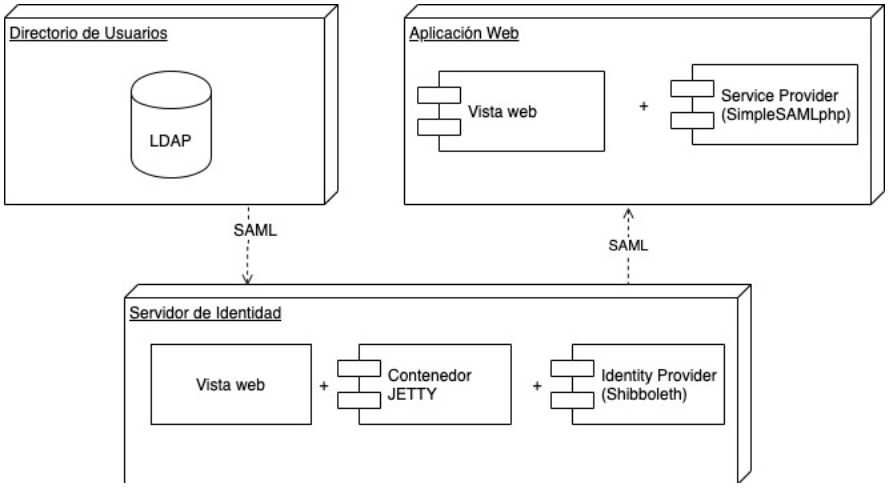



***Ilustración 34*** *Diagrama de despliegue del piloto*[35]

El piloto desplegado está compuesto por las siguientes 3 instancias:

**Directorio de usuarios**: Su componente es un OpenLDAP y es el repositorio de usuarios en producción de la UTP.

**Aplicación web**: Consta de 2 componentes, un sitio web desplegado con Wordpress y una herramienta para federación de servicios llamada SimpleSAMLphp.

**Servidor de identidad**: Conformado por 3 componentes, un proveedor de identidad que se instaló la herramienta para federación de identidad llamada Shibboleth, un contenedor de aplicaciones *JAVA* llamado *JETTY* y un servidor web para publicar la metadata.

---

[35] **Fuente:** Del autor

### 5.4.2 Herramientas utilizadas

**OpenLDAP**: Es una implementación *open source* del protocolo LDAP que incluye SLAPD (Servidor LDAP) y librerías del protocolo (OpenLDAP, 2020). En el caso de la UTP, este ya se encuentra instalado y es usado como directorio de usuarios institucional.

**Wordpress**: Es un sistema de gestión de contenido (CMS sus siglas en inglés) de uso libre. Este permite creación de sitios web y ofrece gran variedad de herramientas que facilitan el desarrollo e implementación de múltiples tecnologías.

**SimpleSAMLphp**: Es una herramienta de uso libre desarrollada en PHP que soporta el uso de varios protocolos de federación de identidad.

**Apache HTTP server**: Es un proyecto de servidor web de uso libre ampliamente usado en ambientes GNU/Linux, UNIX y Windows. Es desarrollado por "APACHE Software foundation".

**JETTY**: Contenedor de aplicaciones JAVA que pertenece a la fundación Eclipse. Es oficialmente soportado por la herramienta Shibboleth utilizada en este proyecto como proveedor de identidad.

**Shibboleth:** Shibboleth es una herramienta de código abierto disponible de forma gratuita, con funcionalidades de SSO, continuamente en desarrollo para satisfacer las necesidades de las federaciones de identidad.

### 5.4.3 Instalación y configuración Proveedor de identidad

El IdP Shibboleth es una aplicación web estándar de Java basada en la especificación Servlet 3.0 y debe ejecutarse en su mayor parte en cualquier contenedor de servlets compatible, la instalación del piloto para la UTP se realizará con el contenedor "JETTY" la cual tiene soporte oficial por el grupo de desarrollo de Shibboleth. El servidor web utilizado es *Apache HTTP server* (Ver **Ilustración 35** Instalación y configuración IdP )

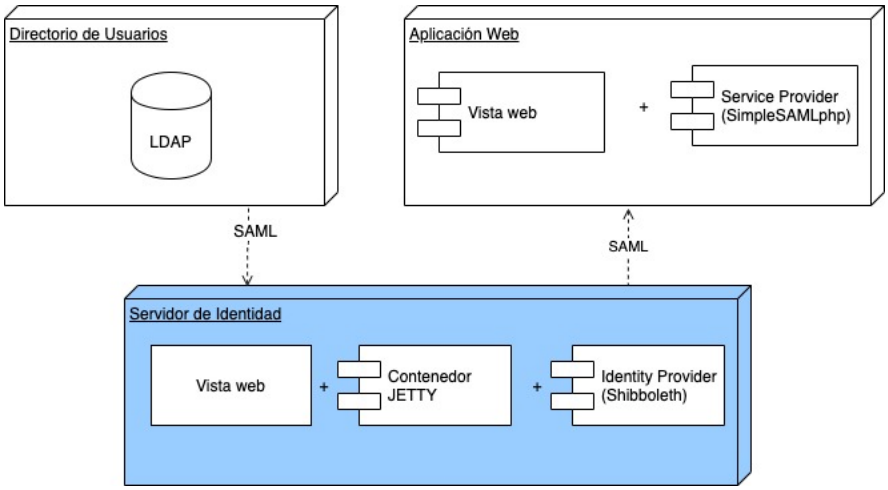



***Ilustración 35*** *Instalación y configuración IdP*[36]

[36] **Fuente:** Del autor

**Configuración de hardware y software del servidor instalado:**

| |
|---|
| •Arquitectura: 64 bits<br>•Sistema operativo: Linux<br>•Memoria RAM: 4GB<br>•Espacio en disco: 80GB<br>•Cantidad de Procesadores: 2 |

El servidor fue ubicado en la zona desmilitarizada de la universidad, se crearon los registros DNS idp.utp.edu.co internos y externos, y se agregaron las reglas permitiendo el acceso por los puertos 80 y 443 desde internet y la LAN de la red de la UTP.

## Instalando servidor web

```
[root@idp ~]# yum install httpd

Package httpd-2.4.37-11.module_el8.0.0+172+85fc1f40.x86_64.
Dependencies resolved.
================================================================================
 Package          Arch       Version                                  Repository      Size
================================================================================
Upgrading:
 httpd            x86_64     2.4.37-16.module_el8.1.0+256+ae790463    AppStream      1.7 M
 httpd-filesystem noarch     2.4.37-16.module_el8.1.0+256+ae790463    AppStream       35 k
 httpd-manual     noarch     2.4.37-16.module_el8.1.0+256+ae790463    AppStream      2.4 M
 httpd-tools      x86_64     2.4.37-16.module_el8.1.0+256+ae790463    AppStream      103 k
 mod_ssl          x86_64     1:2.4.37-16.module_el8.1.0+256+ae790463  AppStream      131 k

Transaction Summary
================================================================================
Install 5 Packages

Total download size: 4.3 M
Is this ok [y/N]: y
```

## Instalando JAVA

En nuestro caso el JAVA no venía preinstalado por lo cual se indican los pasos para su instalación. En caso de tenerlo instalado obviar este paso.

```
[root@idp instaladores]# yum install java

================================================================================
 Package                 Arch       Version                        Repository      Size
================================================================================
Installing:
 java-1.8.0-openjdk      x86_64     1:1.8.0.232.b09-2.el8_1        AppStream      317 k
Upgrading:
 lua-libs                x86_64     5.3.4-11.el8                   BaseOS         118 k
Installing dependencies:
 alsa-lib                x86_64     1.1.9-4.el8                    AppStream      429 k
 copy-jdk-configs        noarch     3.7-1.el8                      AppStream       27 k
 giflib                  x86_64     5.1.4-3.el8                    AppStream       51 k
 java-1.8.0-openjdk-headless x86_64 1:1.8.0.232.b09-2.el8_1        AppStream       33 M
```

```
javapackages-filesystem                noarch          5.3.0-1.module_el8.0.0+11+5b8c10bd          AppStream          30 k
 libXtst                               x86_64          1.2.3-7.el8                                 AppStream          22 k
 lua                                   x86_64          5.3.4-11.el8                                AppStream         193 k
 ttmkfdir                              x86_64          3.0.9-54.el8                                AppStream          62 k
 tzdata-java                           noarch          2019c-1.el8                                 AppStream         189 k
 xorg-x11-fonts-Type1                  noarch          7.5-19.el8                                  AppStream         522 k
 lksctp-tools                          x86_64          1.0.18-3.el8                                BaseOS            100 k
Enabling module streams:
 javapackages-runtime                                  201801

Transaction Summary
================================================================================================================================
Install  12 Packages
Upgrade   1 Package

Total download size: 35 M
Is this ok [y/N]: y
```

## Instalación jetty

Ahora procedemos con la descargar del archivo que contiene los instaladores del contenedor JETTY. El enlace puede ser copiado el sitio oficial https://www.eclipse.org/jetty/download.html

```
[root@idp ~]# cd instaladores/

[root@idp instaladores]# wget https://repo1.maven.org/maven2/org/eclipse/jetty/jetty-distribution/9.3.28.v20191105/jetty-distribution-

9.3.28.v20191105.tar.gz

https://repo1.maven.org/maven2/org/eclipse/jetty/jetty-distribution/9.3.28.v20191105/jetty-distribution-9.3.28.v20191105.tar.gz
Resolving repo1.maven.org (repo1.maven.org)... 151.101.204.209
Connecting to repo1.maven.org (repo1.maven.org)|151.101.204.209|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17700830 (17M) [application/x-gzip]
Saving to: 'jetty-distribution-9.3.28.v20191105.tar.gz'

jetty-distribution-9.3.28.v20191105.tar.gz
100%[==========================================================================================================>] 16.88M  3.42MB/s    in
5.7s

 (2.98 MB/s) - 'jetty-distribution-9.3.28.v20191105.tar.gz' saved [17700830/17700830]



Una vez descargado se procede a descomprimir los archivos



[root@idp instaladores]# tar xvf jetty-distribution-9.3.28.v20191105.tar.gz

jetty-distribution-9.3.28.v20191105/
jetty-distribution-9.3.28.v20191105/webapps/
jetty-distribution-9.3.28.v20191105/bin/
jetty-distribution-9.3.28.v20191105/resources/
jetty-distribution-9.3.28.v20191105/demo-base/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/ROOT/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/ROOT/images/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/9.3.28.v20191105/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/9.3.28.v20191105/css/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/9.3.28.v20191105/css/highlighter/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/9.3.28.v20191105/css/font-awesome/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/9.3.28.v20191105/images/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/9.3.28.v20191105/js/
jetty-distribution-9.3.28.v20191105/demo-base/webapps/doc/9.3.28.v20191105/fonts/
…
```

Para la configuración seguir los pasos publicados en:

https://wiki.shibboleth.net/confluence/display/IDP30/Jetty93

Para este piloto se utilizará un certificado auto firmado. Si la institución cuenta con certificados válidos los puede utilizar y obviar este paso:

**[root@idp ~]# mkdir certificates**

**[root@idp ~]# openssl req -x509 -newkey rsa:4096 -keyout /root/certificates/idp-key-server.key -out /root/certificates/idp-cert-server.crt -nodes -days 1095**

```
Generating a RSA private key
.............++++
.................++++
writing new private key to '/root/certificates/idp-key-server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CO
State or Province Name (full name) []:RISARALDA
Locality Name (eg, city) [Default City]:PEREIRA
Organization Name (eg, company) [Default Company Ltd]:UTP
Organizational Unit Name (eg, section) []:CRIE
Common Name (eg, your name or your server's hostname) []:idp.utp.edu.co
Email Address []:federacion@utp.edu.co
```

**Cambiamos los permisos como se indica:**

**chmod 400 /root/certificates/idp-key-server.key**

**chmod644 /root/certificates/idp-cert-server.cr**

## Instalación *Shibboleth*

Se descarga el archivo instalador del sitio web oficial de *Shibboleth*.

**[root@idp ~]# cd instaladores/**

**[root@idp instaladores]# wget https://shibboleth.net/downloads/identity-provider/3.2.1/shibboleth-identity-provider-3.2.1.tar.gz**

```
https://shibboleth.net/downloads/identity-provider/3.2.1/shibboleth-identity-provider-3.2.1.tar.gz
Resolving shibboleth.net (shibboleth.net)... 108.163.128.190
Connecting to shibboleth.net (shibboleth.net)|108.163.128.190|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 39507368 (38M) [application/x-gzip]
Saving to: ‘shibboleth-identity-provider-3.2.1.tar.gz’

shibboleth-identity-provider-3.2.1.tar.gz   100%[=========================================================================>]  37.68M  11.1MB/s    in 4.1s

(9.16 MB/s) - ‘shibboleth-identity-provider-3.2.1.tar.gz’ saved [39507368/39507368]
```

**Descomprimir el archivo:**

```
[root@idp instaladores]# tar xvf shibboleth-identity-provider-3.2.1.tar.gz
shibboleth-identity-provider-3.2.1/
shibboleth-identity-provider-3.2.1/bin/
shibboleth-identity-provider-3.2.1/bin/lib/
shibboleth-identity-provider-3.2.1/embedded/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/resources/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/etc/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/start.d/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/webapps/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/lib/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/lib/ext/
shibboleth-identity-provider-3.2.1/embedded/jetty-base/lib/logging/
…

[root@idp instaladores]# cd shibboleth-identity-provider-3.2.1/
[root@idp shibboleth-identity-provider-3.2.1]# ./bin/install.sh
```

Ingresar los siguientes datos durante la instalación. Para este piloto se utilizará el dominio idp.utp.edu.co.

- **Installation Directory**: [/opt/shibboleth-idp]
- **Hostname**:idp.[idp.utp.edu.co]
- **SAML EntityID**: [https://idp.utp.edu.co/idp/shibboleth]
- **Attribute Scope**: [localdomain]
- **Backchannel PKCS12 Password**:[ingresar credenciales para el certificado]
- **Cookie Encryption Key Password**:[ingresar credenciales de encripción]

Finalizada la instalación se procede con la importación de las librerías JST para visualizar el *status* del IDP

```
[root@idp shibboleth-identity-provider-3.2.1]# cd /opt/shibboleth-idp/edit-webapp/WEB-INF/lib

[root@idp lib]# wget https://build.shibboleth.net/nexus/service/local/repositories/thirdparty/content/javax/servlet/jstl/1.2/jstl-1.2.jar

https://build.shibboleth.net/nexus/service/local/repositories/thirdparty/content/javax/servlet/jstl/1.2/jstl-1.2.jar
Resolving build.shibboleth.net (build.shibboleth.net)... 174.142.198.207
Connecting to build.shibboleth.net (build.shibboleth.net)|174.142.198.207|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 414240 (405K) [application/java-archive]
Saving to: 'jstl-1.2.jar'
```

```
jstl-1.2.jar
100%[=========================================================================================================================>] 404.53K   531KB/s    in
0.8s

2020-02-06 12:48:11 (531 KB/s) - ‘jstl-1.2.jar’ saved [414240/414240]

Cambiar el propietario para habilitar al usuario Jetty acceder a los siguientes directorios:

[root@idp lib]# cd ..

[root@idp WEB-INF]# chown -R jetty logs/ metadata/ credentials/ conf/ system/ war/
```

## Configurar SSL en el servidor web para el contenedor (Jetty front-end)

1. Modificar los siguientes parámetros del archivo /etc/httpd/sites-available/default-ssl.conf:

```
<IfModulemod_ssl.c>
        SSLStaplingCache shmcb:/var/run/ocsp(128000)

  <VirtualHost_default_:443>
        ServerName  idp.utp.edu.co:443
        federacion@utp.edu.co
        DocumentRoot            /var/www/html
        ...

        SSLEngineOn
        SSLProtocolAll -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
        SSLCipherSuite"EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH"
        SSLHonorCipherOrder on

        # Disable SSL Compression
        SSLCompression Off

        # OCSP Stapling, only in httpd/apache >= 2.3.3
        SSLUseStapling on
        SSLStaplingResponderTimeout 5
        SSLStaplingReturnResponderErrors off

        # Enable HTTP Strict Transport Security with a 2 year duration
        Header always set Strict-Transport-Security "max-age=63072000;includeSubDomains;preload"
        ...
        SSLCertificateFile/root/certificates/idp-cert-server.crt
        SSLCertificateKeyFile/root/certificates/idp-key-server.key
        SSLCertificateChainFile/root/certificates/DigiCertCA.pem
        ...
  </VirtualHost>
</IfModule>
```

2. Activar los módulos proxy_http, SSLy headers del servidor web

```
root@idp:~# a2enmod proxy_http ssl headers alias include negotiation

root@idp:~# a2ensite default-ssl.conf

root@idp:~# systemctl restart httpd.service
```

3. Configurar el servidor web para abrir el puerto 80 de forma local:

```
Listen127.0.0.1:80
<IfModulessl_module>
        Listen 443
</IfModule>

<IfModulemod_gnutls.c>
        Listen 443
</IfModule>
```

4. Configurar el servidor web para redireccionar todo a https

```
<VirtualHost*:80>
        ServerName "idp.utp.edu.co"
        Redirect "/" https://idp.utp.edu.co/
</VirtualHost>
```

## Habilitando Jetty desde el servidor web

1. Crear archivo de configuración para IdP

/etc/httpd/conf.d/idp.conf

```
<IfModule mod_proxy.c>
        ProxyPreserveHost On
        RequestHeader set X-Forwarded-Proto "https"
        ProxyPass /idp http://localhost:8080/idp retry=5
        ProxyPassReverse/idp http://localhost:8080/idp retry=5
```

```
  <Location /idp>
        Require all granted
  </Location>
</IfModule>
```

2. Reiniciar el servicio web

```
root@idp:~# systemctl restart httpd.service
```

3. Configurar el descriptor de contexto en el contenedor para el IdP

/opt/jetty/webapps/idp.xml

```
<Configure class="org.eclipse.jetty.webapp.WebAppContext">
  <Set name="war"><SystemProperty name="idp.home"/>/war/idp.war</Set>
  <Set name="contextPath">/idp</Set>
  <Set name="extractWAR">false</Set>
  <Set name="copyWebDir">false</Set>
  <Set name="copyWebInf">true</Set>
</Configure>
```

4. Reiniciar el Jetty

```
root@idp:~# systemctl restart jetty.service
```

**Configuración de *Shibboleth* para que conozca los parámetros del servidor *LDAP* y pueda autenticar usuarios**.

Se muestran los parámetros que deben ser ajustados:

/opt/shibboleth-idp/conf/ldap.properties

```
# Servidor LDAP de UTP y el puerto a través del cual escucha peticiones
idp.authn.LDAP.ldapURL                  = ldap://ldap.utp.edu.co:778

# Arbol de usuarios de la institución
idp.authn.LDAP.baseDN                   = ou=Usuarios,dc=utp
idp.authn.LDAP.subtreeSearch             = true

# Filtro que define con qué parámetro se van a autenticar los usuarios
idp.authn.LDAP.userFilter               = (mail={user})

# Credenciales para realizar consultas al servidor LDAP
idp.authn.LDAP.bindDN                   = uid=XXXX,dc=utp
idp.authn.LDAP.bindDNCredential          = XXXX

# Arbol para consultar la autenticación del usuario
idp.authn.LDAP.dnFormat                 = uid=%s,ou=Usuarios,dc=utp

# Atributos que debe devolver la consulta LDAP al directorio
idp.attribute.resolver.LDAP.returnAttributes    = cn,mail
```

## Habilitar SAML v2 y deshabilitar SAML v1.x en el archive idp-metadata.xml

/opt/shibboleth-idp/metadata/idp-metadata.xml

**En la sección <EntityDescriptor"> agregue:**

-xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"

-xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"

**En la sección <IDPSSODescriptor>:**

**–de la lista"protocolSupportEnumeration" elimine:**

-urn:oasis:names:tc:SAML:1.1:protocol

-urn:mace:shibboleth:1.0

**–Elimine el endpoint:**

<ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"

Location="https://idp.example.org:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/>

(ymodifique el"index value" of del siguiente a“1”)

**–Elimine elendpoint:**

<NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>

**–Añada debajo de la línea:**

<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>

**Esta línea:**

<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>

**(porque el IdP instalado con esta guía libera los ID de nombre de SAML persistentes)**

**-Elimine el endpoint:**

<SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"

Location="https://idp.example.org/idp/profile/Shibboleth/SSO"/>

**-Elimine todos los":8443" de la URL actual (ya que el puerto no se va a usar)**

**<AttributeAuthorityDescriptor>Section:**

**–De la lista"protocolSupportEnumeration" reemplace el valor de:**

-urn:oasis:names:tc:SAML:1.1:protocol

**Con**

-urn:oasis:names:tc:SAML:2.0:protocol

**-Elimine el comentario de:**

<AttributeService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

Location="https://idp.example.org/idp/profile/SAML2/SOAP/AttributeQuery"/>

**-Elimine el endpoint:**

<AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"

Location="https://idp.example.org:8443/idp/profile/SAML1/SOAP/AttributeQuery"/>

**Eliminar todos los ":8443" de la URL actual (ya que el puerto no se va a usar)**

- La metadata del IdP configurado puede ser consultada en la URL

  https://idp.utp.edu.co/idp/shibboleth

  Esta metadata debe ser agregada al IdP de RENATA. Correo de contacto tecnico@renata.edu.co

- Ahora se agregan los Metadata-Providers

Se descarga la metadata del sitio web de RedClara

```
cd /opt/shibboleth-idp/metadata/

wget https://nrenadmin.redclara.net/Metadata-dev/metadata-sps-dev.xmlw

get https://nrenadmin.redclara.net/Metadata-Elcira/metadata-elcira-sps.xml

chown jetty:root metadata-elcira-sps.xml

chown jetty:root metadata-sps-dev.xml
```

Y se referencia en el metadata-providers.xml

/opt/shibboleth-idp/conf/metadata-providers.xml

```
<MetadataProvider id="MDS-Edugain" xsi:type="FileBackedHTTPMetadataProvider"
                  metadataURL="http://mds.edugain.org/"
                  backingFile="%{idp.home}/metadata/mds-edugain.xml">
        <MetadataFilter xsi:type="ChainingFilter">
          <MetadataFilter xsi:type="EntityRoleWhiteList">
            <RetainedRole>md:SPSSODescriptor</RetainedRole>
          </MetadataFilter>
        </MetadataFilter>
    </MetadataProvider>


  <MetadataProvider id="FedClaradev"
              xsi:type="FileBackedHTTPMetadataProvider"
              metadataURL="https://nrenadmin.redclara.net/Metadata-dev/metadata-sps-dev.xml"
              backingFile="%{idp.home}/metadata/metadata-sp-FedCLARA-dev.xml">
    <MetadataFilter xsi:type="ChainingFilter">
        <MetadataFilter xsi:type="EntityRoleWhiteList">
            <RetainedRole>md:SPSSODescriptor</RetainedRole>
        </MetadataFilter>
    </MetadataFilter>
  </MetadataProvider>
```

- Se reinicia *Shibboleth*

```
root@idp:~# cd /opt/shibboleth-idp/bin
root@idp:/opt/shibboleth-idp/bin#./reload-service.sh -id shibboleth.MetadataResolverService
```

- Ahora se descarga el archivo *attribute-filter.xml* con los atributos definidos previamente por RENATA

```
root@idp:~# wget https://www.renata.edu.co/idp-conf/attribute-filter.xml -O /opt/shibboleth-idp/conf/attribute-filter.xml
```

Volver a cargar el servicio con ID shibboleth.AttributeFilterService para actualizar la configuración de los filtros

```
root@idp:~# cd /opt/shibboleth-idp/bin./reload-service.sh -id shibboleth.AttributeFilterService
```

Una vez realizadas las anteriores configuraciones y se haya verificado que por parte de RENATA han agregado la *metadata* del IdP instalado, se debe esperar 24 horas aproximadamente para verificar que eduGAIN ya incluye el IdP de la institución. Ver **Ilustración 36**

La verificación se puede realizar a través de un validador que tiene publicado eduGAIN y cuya URL es https://technical.edugain.org/validator2

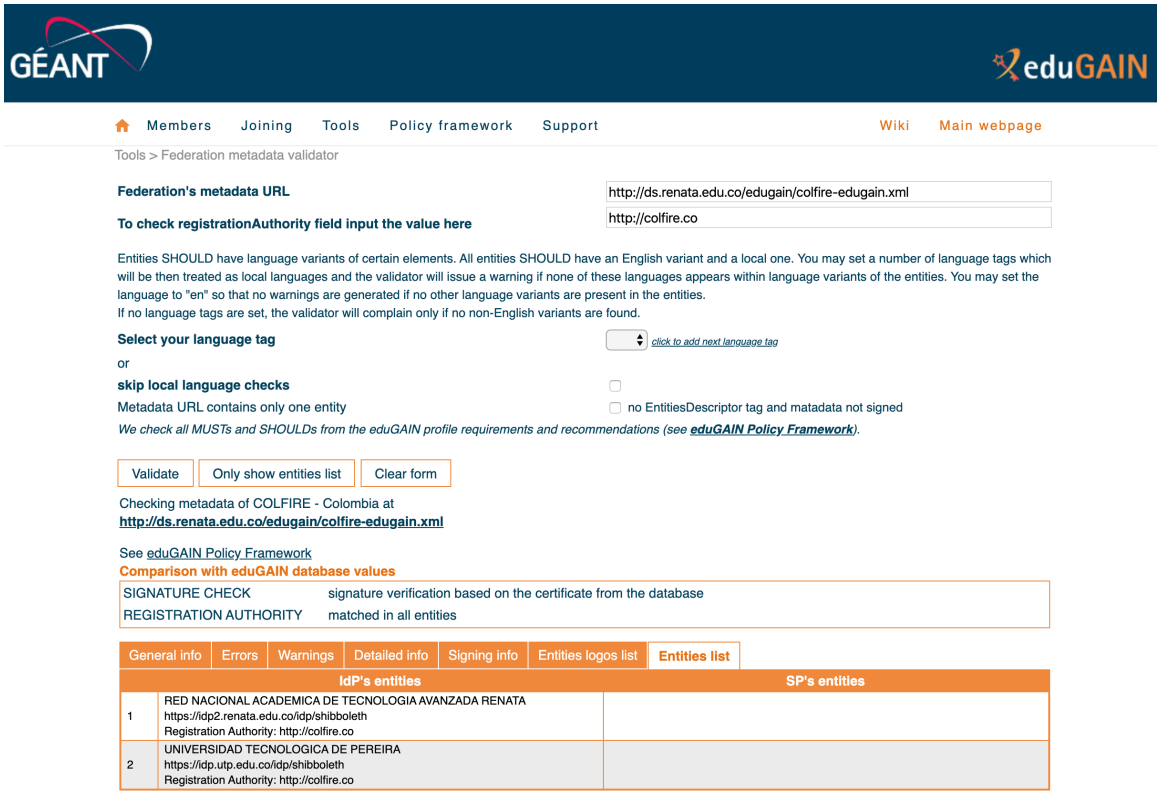



***Ilustración 36*** *Validador metadata eduGAIN*[37]

El 25 de septiembre del año 2019 se culminó con éxito la configuración y publicación del IdP de la Universidad Tecnológica de Pereira en eduGAIN a través de la federación de Colombia llamada COLFIRE. La UTP a febrero de 2020 continúa siendo la única universidad de Colombia cuyos usuarios pueden acceder a los servicios publicados en las instituciones de más de 60 países que pertenecen a eduGAIN.

[37] Fuente: ("eduGAIN – enabling worldwide access," 2020)

### 5.4.4 Instalación y configuración Service Provider

A continuación se presenta la instalación y configuración del servidor de aplicación web.

(Ver **Ilustración 37**)

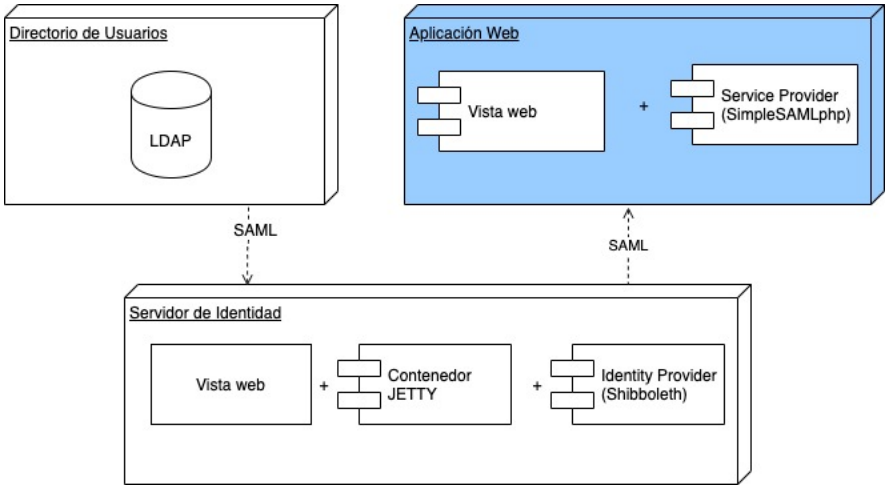



***Ilustración 37*** *Instalación proveedor de servicios*[38]

**Configuración de hardware y software del servidor instalado:**

| |
|---|
| •Arquitectura: 64 bits<br>•Sistema operativo: Linux<br>•Memoria RAM: 8GB<br>•Espacio en disco: 32GB<br>•Cantidad de Procesadores: 2 |

[38] **Fuente:** Del autor

El servidor fue ubicado en la zona desmilitarizada de la universidad, se crearon los registros DNS sp.utp.edu.co internos y externos, y se agregaron las reglas permitiendo el acceso por los puertos 80 y 443 desde internet y la LAN de la red de la UTP.

## Instalando servidor web

```
[root@idp ~]# yum install httpd

Package httpd-2.4.37-11.module_el8.0.0+172+85fc1f40.x86_64.
Dependencies resolved.
================================================================================
 Package          Arch       Version                                  Repository      Size
================================================================================
Upgrading:
 httpd            x86_64     2.4.37-16.module_el8.1.0+256+ae790463    AppStream      1.7 M
 httpd-filesystem noarch     2.4.37-16.module_el8.1.0+256+ae790463    AppStream       35 k
 httpd-manual     noarch     2.4.37-16.module_el8.1.0+256+ae790463    AppStream      2.4 M
 httpd-tools      x86_64     2.4.37-16.module_el8.1.0+256+ae790463    AppStream      103 k
 mod_ssl          x86_64     1:2.4.37-16.module_el8.1.0+256+ae790463  AppStream      131 k

Transaction Summary
================================================================================
Install 5 Packages

Total download size: 4.3 M
Is this ok [y/N]: y
```

## Instalando SimpleSAMLphp

Se descarga la última versión de la URL https://simplesamlphp.org/download

```
[root@sp ~]# mkdir /instaladores/
[root@sp ~]# wget https://github.com/simplesamlphp/simplesamlphp/releases/download/v1.18.3/simplesamlphp-1.18.3.tar.gz
[root@sp ~]# tar zxf simplesamlphp-1.18.3.tar.gz
[root@sp instaladores]# mv simplesamlphp-1.18.3 /var/simplesamlphp/
```

Configurando servidor web

```
[root@sp instaladores]# cd /etc/httpd/conf.d/

Configuración virtual host
[root@sp conf.d]# vi vhost.conf
  <VirtualHost *>
        ServerName sp.utp.edu.co
        DocumentRoot /var/www/sp

        SetEnv SIMPLESAMLPHP_CONFIG_DIR /var/simplesamlphp/config

        Alias /simplesaml /var/simplesamlphp/www

        <Directory /var/simplesamlphp/www>
           Require all granted
        </Directory>
  </VirtualHost>

Configuración SSL
[root@sp conf.d]# vi ssl.conf

        ServerName sp.utp.edu.co
        DocumentRoot /var/www/sp

        SetEnv SIMPLESAMLPHP_CONFIG_DIR /var/simplesamlphp/config
```

```
Alias /simplesaml /var/simplesamlphp/www

<Directory /var/simplesamlphp/www>
    Require all granted
</Directory>
```

Luego se modifica el archivo config.php en /var/simplesamlphp/config las siguientes líneas

***Poner la ruta web a la instalación de SimpleSAML***

'baseurlpath' => 'https://sp.utp.edu.co/simplesaml/',

***Cambiar clave de acceso***

'auth.adminpassword' => 'XXXXX',

***Generar código HASH utilizado por algunas funciones internas de SimpleSAMLphp***

[root@sp config]# tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo

***El resultado lo agregamos en la siguiente línea***

'secretsalt' => 'a0zkqb9yjq1iwevapa2446zv8c89exyz',

***Luego información de contacto***

'technicalcontact_name' => 'Administrator',
'technicalcontact_email' => 'federacion@utp.edu.co',

Ahora se verifica que se tenga acceso vía web (Ver **Ilustración 38** SimpleSAMLphp instalado)

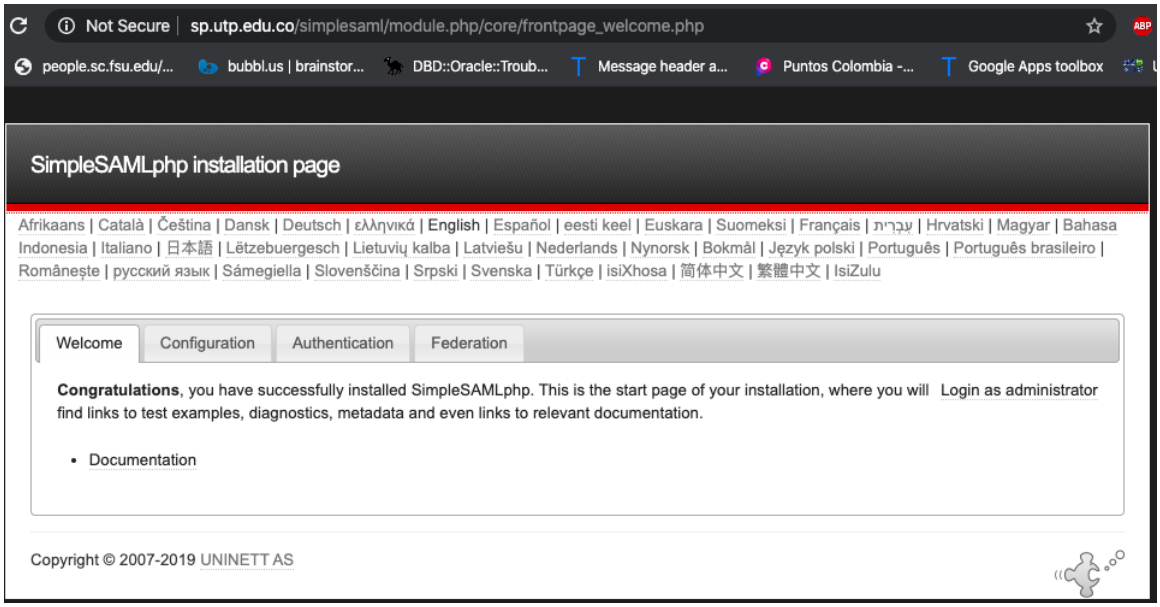



***Ilustración 38*** *SimpleSAMLphp instalado*[39]

## Configuración SimpleSAMLphp como proveedor de servicio

Generar certificado digital para el SP

```
[root@sp ~]# cd /var/simplesamlphp/cert
[root@sp cert]#openssl req -newkey rsa:3072 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pem

Generating a RSA private key
.....................................................+++++
.......+++++
writing new private key to 'saml.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CO
State or Province Name (full name) []:Risaralda
Locality Name (eg, city) [Default City]:Pereira
Organization Name (eg, company) [Default Company Ltd]:UTP
Organizational Unit Name (eg, section) []:ADMRED
Common Name (eg, your name or your server's hostname) []:SP
Email Address []:federacion@utp.edu.co
```

Se modifica el archivo authsources.php

```
[root@sp ~]# cd /var/simplesamlphp/config
[root@sp config]# vi authsources.php
```

***Para el piloto el nombre del servicio a federar será "default-SP". Se verifican los nombres de la llave pública y privada del certificado.***

[39] **Fuente:** Del autor

```
'default-sp' => [
    'saml:SP',
    'privatekey' => 'saml.pem',
    'certificate' => 'saml.crt',
```

Se agrega la metadata del IdP previamente instalado al archivo saml20-idp-remote.php

```
[root@sp config]# cd /var/simplesamlphp/metadata
[root@sp metadata]# vi saml20-idp-remote.php

Configuramos la URL de la metadata del IdP

        $metadata['https://idp.utp.edu.co/idp/shibboleth'] = [
            'certificate'          => 'saml.pem',
        ];
```

Se debe convertir la metadata del IdP al formato de SimpleSAMLphp. Para lograr esto se debe ir a la herramienta que está en https://sp.utp.edu.co/simplesaml/admin/metadata-converter.php. (Ver **Ilustración 39**)

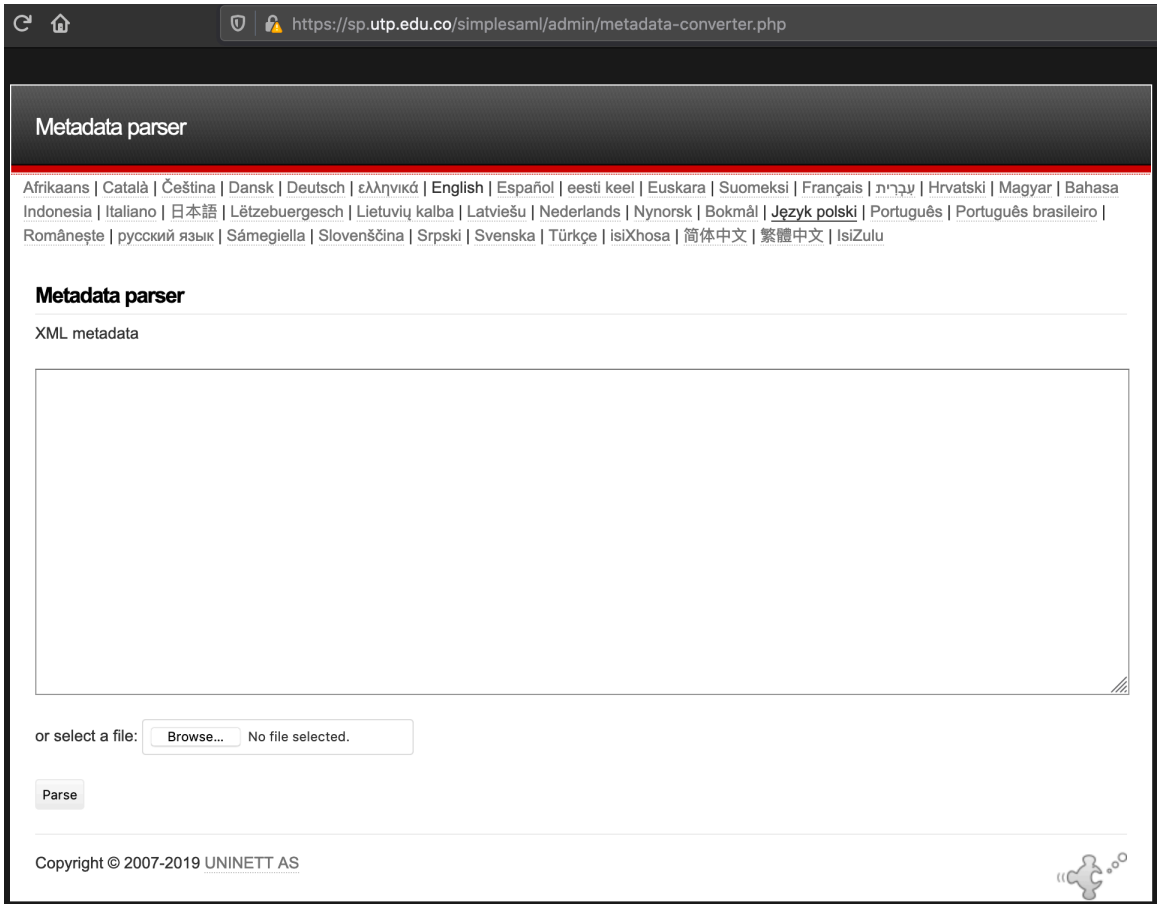



***Ilustración 39*** *Convertidor Metadata*[40]

Se copia allí la metadata del IdP que está en la URL https://idp.utp.edu.co/idp/shibboleth

(Ver **Ilustración 40**)

[40] **Fuente:** Del autor

https://idp.utp.edu.co/idp/shibboleth

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<!--
        UTP This is example metadata only. Do *NOT* supply it as is without review,
        and do *NOT* provide it in real time to your partners.

        This metadata is not dynamic - it will not change as your configuration changes.
 -->
<EntityDescriptor entityID="https://idp.utp.edu.co/idp/shibboleth">
  <Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://colfire.co" registrationInstant="2014-01-01T00:00:00Z">
      <mdrpi:RegistrationPolicy xml:lang="en"> http://colfire.co/?page_id=55</mdrpi:RegistrationPolicy>
      <mdrpi:RegistrationPolicy xml:lang="es"> http://colfire.co/?page_id=55</mdrpi:RegistrationPolicy>
    </mdrpi:RegistrationInfo>
  </Extensions>
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>
      <shibmd:Scope regexp="false">utp.edu.co</shibmd:Scope>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="en"> UNIVERSIDAD TECNOLOGICA DE PEREIRA </mdui:DisplayName>
        <mdui:DisplayName xml:lang="es"> UNIVERSIDAD TECNOLOGICA DE PEREIRA </mdui:DisplayName>
        <mdui:Description xml:lang="en">Login to acces to all our services!</mdui:Description>
        <mdui:Description xml:lang="es">
          ¡Inicia sesión para acceder a todos tus Servicios de Tecnología Avanzada
        </mdui:Description>
        <mdui:Logo height="80" width="80">
          https://www.utp.edu.co/assets/img/escudos/identificadorw.png
        </mdui:Logo>
```

***Ilustración 40*** *Metadata IdP*[41]

Una vez realizada la conversión, se copia la nueva metadata al archivo authsources.php

```
$metadata['https://idp.utp.edu.co/idp/shibboleth'] = array (
  'entityid' => 'https://idp.utp.edu.co/idp/shibboleth',
  'description' =>
  array (
    'es' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
    'en' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
  ),
  'OrganizationName' =>
  array (
    'es' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
    'en' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
  ),
  'name' =>
  array (
    'en' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
    'es' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
  ),
  'OrganizationDisplayName' =>
  array (
    'es' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
    'en' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
  ),
  'url' =>
  array (
    'es' => 'http://www.utp.edu.co',
    'en' => 'http://www.utp.edu.co',
  ),
  'OrganizationURL' =>
  array (
    'es' => 'http://www.utp.edu.co',
    'en' => 'http://www.utp.edu.co',
  ),
  'contacts' =>
```

[41] **Fuente:** Del autor

```
  array (
    0 =>
    array (
      'contactType' => 'technical',
      'surName' => '
Administracion de Redes y Seguridad de la Informacion
',
      'emailAddress' =>
      array (
        0 => 'mailto:admred@utp.edu.co',
      ),
    ),
  ),
  'metadata-set' => 'saml20-idp-remote',
  'SingleSignOnService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
      'Location' => 'https://idp.utp.edu.co/idp/profile/SAML2/POST/SSO',
    ),
    1 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign',
      'Location' => 'https://idp.utp.edu.co/idp/profile/SAML2/POST-SimpleSign/SSO',
    ),
    2 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://idp.utp.edu.co/idp/profile/SAML2/Redirect/SSO',
    ),
  ),
  'SingleLogoutService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://idp.utp.edu.co/idp/profile/SAML2/Redirect/SLO',
    ),
    1 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
      'Location' => 'https://idp.utp.edu.co/idp/profile/SAML2/POST/SLO',
    ),
    2 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign',
      'Location' => 'https://idp.utp.edu.co/idp/profile/SAML2/POST-SimpleSign/SLO',
    ),
    3 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:SOAP',
      'Location' => 'https://idp.utp.edu.co:8443/idp/profile/SAML2/SOAP/SLO',
    ),
  ),
  'ArtifactResolutionService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:SOAP',
      'Location' => 'https://idp.utp.edu.co/idp/profile/SAML2/SOAP/ArtifactResolution',
      'index' => 1,
    ),
  ),
  'NameIDFormats' =>
  array (
    0 => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',
    1 => 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',
  ),
  'keys' =>
  array (
    0 =>
    array (
      'encryption' => false,
      'signing' => true,
      'type' => 'X509Certificate',
      'X509Certificate' => '
MIIDJDCCAgygAwIBAgIVAKecJi9IXIEMhFFYVOW03eA3D1y8MA0GCSqGSIb3DQEB CwUAMBkxFzAVBgNVBAMMDmlkcC51dHAuZWR1LmNvMB4XDTE4MTAxMDIxMTQyMFoX
DTM4MTAxMDIxMTQyMFowGTEXMBUGA1UEAwwOaWRwLnV0cC5lZHUuY28wggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCBi7EGQ/UPWazB7
w+jPRSgLvTFaaN8 D1PNub3+b9i7Dwdj0nfUTbZ1gZt2cSJ6g4QYTkrcLVVrKaZmTdwmh/btjoXDy9YF OFJpJhN3BMs1lPRP0BWlPjZElm5ujTsAizmVo5llr3Tac6cOm+dFekhUhayz49aP
ehXjsIs9ychvWtG8B0QCJn0vTJWi935JS4diyiwnXNiBrPY2gXpD7bIES/cRfOD5 sF0oxogna2r5UgLqEjhchagkxSd7D//vg
GywbooH1g8Nsza92Ro13rHNyPfAKg1q m3QxcXexnnmGbHVHP0Bf9nWw55OpIR7/YJxMcXqAF3eOQegi0EcwzQwfAgMBAAGj
YzBhMB0GA1UdDgQWBBQfs7z9SS3r8arkNX9W3HBqCt70JDBABgNVHREEOTA3gg5p ZHAudXRwLmVkdS5jb4YlaHR0cHM6Ly9pZHAudXRwLmVkdS5jby9pZHAvc2hpYmJv
bGV0aDANBgkqhkiG9
w0BAQsFAAOCAQEAaJZRsgfOqAahKk6/G/7V9ejKGi2/85ME F5G7bH87bSkEhiJS6ScSGzIxFWDfD3SFevu2D1odl8zl+FU1O81xJpe+/FLVl9oS
r63RXiAvPhujO36XkYTu4kh4AfaMV+rB7OO7xu5zSqkWkoISoiZIkOqNASTDGOTf OE5YdZfMpZ/LDYeiSEhbmGoT5iYYleD2p4V5YmsSrTLdcxpfACjQ27ZkrfH+8Yfk p
He8rqZGEXVd957HBDrKDjwnftFzrdc7FosjWbg3dPRzEX9BBG7gb6rRG8RV14Vy jg/6z17Z9D7KTj2XQOSFn7qYYa9Hbo11vpB1YclMzeWXlJgVdb6U0A==
',
    ),
    1 =>
    array (
      'encryption' => false,
      'signing' => true,
      'type' => 'X509Certificate',
      'X509Certificate' => '
MIIDlzCCAgugAwIBAgIUIxnj+22YsujrN6oBLlaixDfQl3wwDQYJKoZIhvcNAQEL BQAwGTEXMBUGA1UEAwwOaWRwLnV0cC5lZHUuY28wHhcNMTgxMDEwMjExNDE5WhcN
MzgxMDEwMjExNDE5WjAZMRcwFQYDVQQDDA5pZHAudXRwLmVkdS5jbzCCASIwDQYJ KoZIhvcNAQEBBQADggEPADCCAQoCggEBALzT2uT87/Ykg9Ue0
gZ3CzeE+sm20FiX k3D0QRcxpdekCoCSAqirg7e5TMM85B7KZXNPiGAM6AaX4XIIEm31EyCA+LV4PdK2 81u/746x1R0MzqzyNsqIBAQvRmNfH+fwOl0oetOO4pg0HP/kG3pH3k4PNxcy9KYn
EpuBDWwrXunX+RANWVroljA3uMIrAvEIsgU4RmwsCrKpVIjSdkTypsvPBJzcNAmZ +P8bjk/Q5dUcsoBnz0hkJN0+C1tBlazG
JtoI88ws60Iaw80BXBP+SpaHT20Vmzj 6m4RpATaVfR9DVyVF87FMrgt8+mUykPE15MGQQLoYCyvY5wnbsqtcBcCAwEAAaNj
MGEwHQYDVR0OBBYEFHcNSMaWWmHEsQ7whQ/4pqigpCisMEAGA1UdEQQ5MDeCDmlk cC51dHAuZWR1LmNvhiVodHRwczovL2lkcC51dHAuZWR1LmNvL2lkcC9zaGliYm9s
ZXRoMA0GCSqGSIb3D
QEBCwUAA4IBAQAIf+k5RqNxFwViElOZRUcoq+gZ5nVSsthp qBKHbf473+gTidzuNpohPQrym0G7nRoIQ6YpKqHHJXI0cqjhdAcR8ABuxO5lfjx8
1YIozgLUQz2bMOI+aArot2+ZlaCwBzIqW/yFKViNUwX2v9YZ6ofENkEY0hT2I3sL GYwcH1c2NhgS5pUv4aXcJ44kQqiB+jR73ETMbxsiGzi5t5i8tlQn43amxYCnNes4 h
YR945D0UWismNom+6cMWrapfKb0cAUt/xgU67sy7X9IszbUyP2vCt4Rq9VZ1B6D 5+tYiwHRiVfwbJqGwHoERXj+RwyN/5sWUva4wwAmbWF0zemHVnEn
',
    ),
    2 =>
    array (
      'encryption' => true,
      'signing' => false,
```

```
      'type' => 'X509Certificate',
      'X509Certificate' => '
MIIDIzCCAgugAwIBAgIUGRzHM2i1VbINgydFBnWtY+qr7P4wDQYJKoZIhvcNAQEL BQAwGTEXMBUGA1UEAwwOaWRwLnV0cC5lZHUuY28wHhcNMTgxMDEwMjExNDIwWhcN
MzgxMDEwMjExNDIwWjAZMRcwFQYDVQQDDA5pZHAudXRwLmVkdS5jbzCCASIwDQYJ KoZIhvcNAQEBBQADggEPADCCAQoCggEBAM2qb7otqLojtznJU
YqN5cnX51HHg4ma axe6THBG890OMaOqewXN+1qQra8jd6iQM2dRy7Wv+N1l48y7s1wRg8XSiliaUdnG h39PnYorUhcONv+Tr2BFe7to4HHB0v5afsQosjVbUgT/becBQNxT2quyAPhxb9i8
hcqkYYi3rbHDsLnUzQrWE8gOmZqw6dnPNbLLCr5scPO/VThnfeKaptP1wphOVKP6 8tuqMIzwuU3BVf9Gy6zF+bqSDDQ+WDD8C
X3lzbBolh1BsCr5Vg65MFJC5E9tEnWP L1LATBQ1BrSGbqF/nrzHWdhgZf90K6+VGpWnggzKmOICkGjP/AvtrUcCAwEAAaNj
MGEwHQYDVR0OBBYEFCS9ZVW0EarjyhqUxkFDPpHdsPiTMEAGA1UdEQQ5MDeCDmlk cC51dHAuZWR1LmNvhiVodHRwczovL2lkcC51dHAuZWR1LmNvL2lkcC9zaGliYm9s
ZXRoMA0GCSqGSIb3D
QEBCwUAA4IBAQCj+6SNf4pGwMk8wuT6QDluoMsb6XKt9URg fnAn3zxfNeuNmcg1vYJvYSgfjNzE3KObakcCwgdxKSrwvGuxnWxXza/k2z78n7U6
VNdk1eY8gRmD5YHLDIf05ecLU4/R5s4zJ6Y1gO7evgK9oRG9TkkgUNqYwA/+K9pe yQ373Y9l7kS0UjEXXFb+w1SmzoNO15HMwTwx7WerG0/WqT4buMiys56LKomFUaT9 8
9e6y7p/FTTzVtFJ1w3eIwcekNHJl5HuyGsQpyJwA7//EgoQlLRMYWFLUuKuplAv VjhYH4ZGszKMrf9+CPrR0dmCwLgIjA2rIPrs/v8Bz7Lg1Tf/Um0
'
    ),
  ),
  'scope' =>
  array (
    0 => 'utp.edu.co',
  ),
  'RegistrationInfo' =>
  array (
    'registrationAuthority' => 'http://colfire.co',
  ),
  'UIInfo' =>
  array (
    'DisplayName' =>
    array (
      'en' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
      'es' => 'UNIVERSIDAD TECNOLOGICA DE PEREIRA',
    ),
    'Description' =>
    array (
      'en' => 'Login to acces to all our services!',
      'es' => '¡Inicia sesión para acceder a todos tus Servicios de Tecnología Avanzada',
    ),
    'InformationURL' =>
    array (
    ),
    'PrivacyStatementURL' =>
    array (
    ),
    'Logo' =>
    array (
      0 =>
      array (
        'url' => '
https://www.utp.edu.co/assets/img/escudos/identificadorw.png
',
        'height' => 80,
        'width' => 80,
      ),
    ),
  ),
);
```

El siguiente paso es configurar en el IdP la metadata del proveedor de servicios, en este caso SimpleSAMLphp

Se toma la metadata del SP en la pestaña “Federation” (Ver **Ilustración 41**)

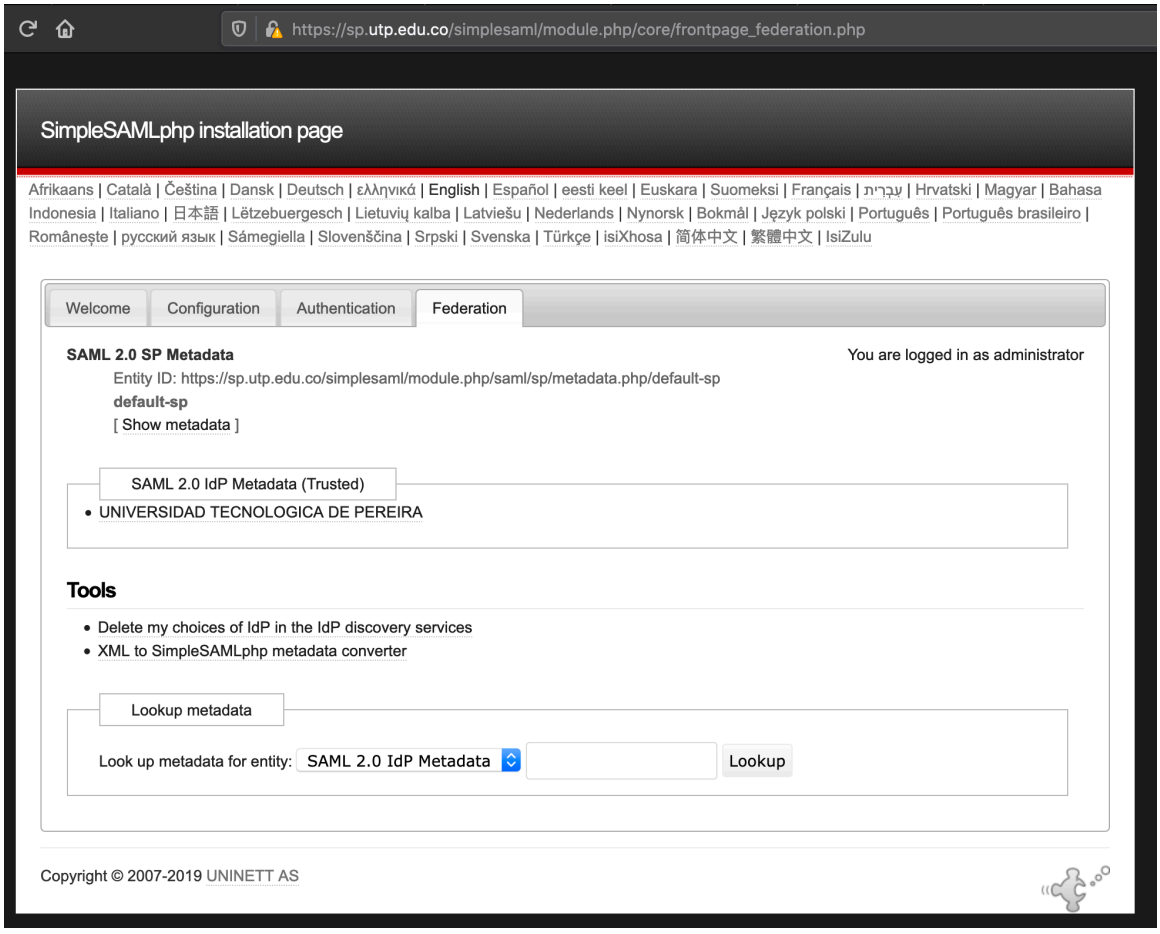



***Ilustración 41*** *Metadata SP*[42]

Se referencia en el archivo metadata-providers.xml

*Copiamos la metadata en el archivo sputp-metadata.xml ubicado en la ruta /opt/shibboleth-idp/metadata*
*Luego la referenciamos en el archivo metadata-providers.xml*

root@idp:~# cd /opt/shibboleth-idp/conf/
root@idp:/opt/shibboleth-idp/conf# vi metadata-providers.xml

Allí agregamos las siguientes líneas:

```
<MetadataProvider id="default-sp"
                  xsi:type="FileBackedHTTPMetadataProvider"
                  metadataURL="https://sp.utp.edu.co/simplesaml/module.php/saml/sp/metadata.php/default-sp"
                  backingFile="%{idp.home}/metadata/sputp-metadata.xml">
    <MetadataFilter xsi:type="ChainingFilter">
        <MetadataFilter xsi:type="EntityRoleWhiteList">
            <RetainedRole>md:SPSSODescriptor</RetainedRole>
        </MetadataFilter>
    </MetadataFilter>
</MetadataProvider>
```

[42] **Fuente:** Del autor

Por último, es necesario reiniciar el IdP.

```
root@idp:/opt/shibboleth-idp/bin# ./reload-service.sh -id shibboleth.MetadataResolverService
```

Ahora se verifica la autenticación desde el proveedor de servicios en la pestaña "*Test authentication sources*", haciendo clic en el enlace "default-sp" (Ver **Ilustración 42** Verificando el IdP desde el SP).

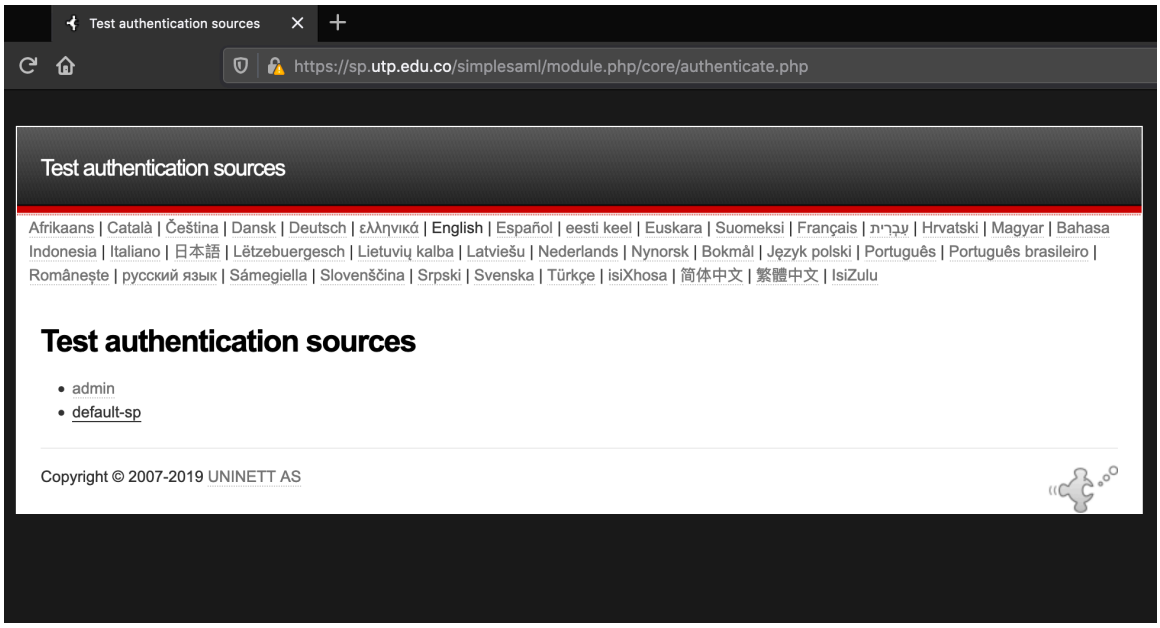



***Ilustración 42*** *Verificando el IdP desde el SP*[43]

[43] **Fuente:** Del autor

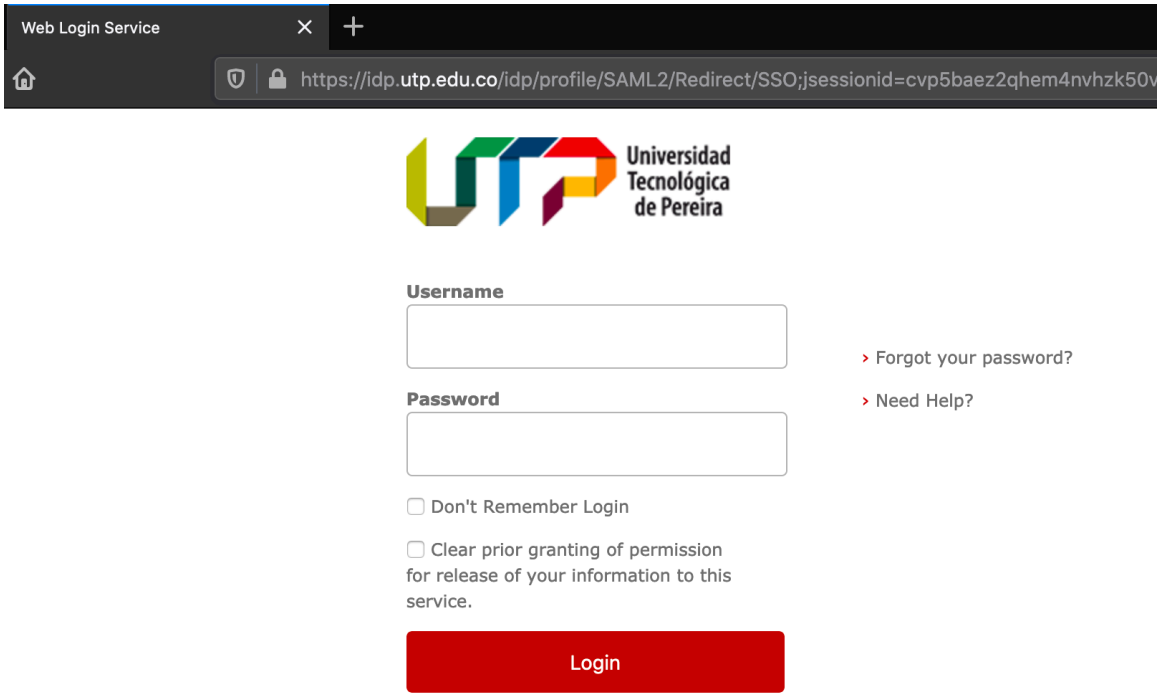



***Ilustración 43*** *Comunicación entre el SP e IdP exitosa*[44]

En la **Ilustración 43** se puede identificar que el SP y el IdP quedaron correctamente configurados.

### 5.4.5 Diagrama de red completo del piloto implementado en la UTP

En la **Ilustración 44** se muestra la topología de red del piloto implementado.

[44] **Fuente:** Del autor

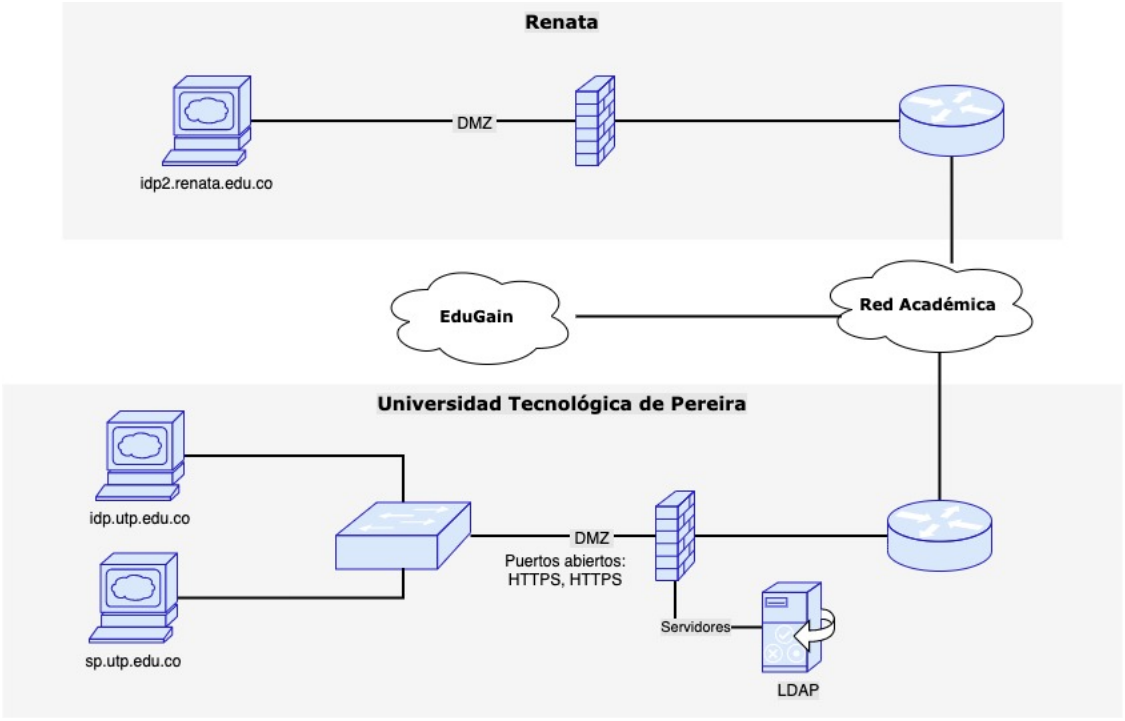



***Ilustración 44*** *Diagrama de red del piloto*[45]

Los servidores donde fueron instalados el SP y el IDP, están ubicados en la zona desmilitarizada de la UTP. Se hace uso del servidor LDAP existente para la autenticación de los usuarios institucionales.

La UTP hace parte de la red nacional académica de tecnología avanzada RENATA, a través de la cual se tiene acceso a la federación de Colombia COLFIRE. El IdP ubicado en RENATA está federado en la red interfederada eduGAIN.

[45] **Fuente:** Del autor

# 6 CUMPLIMIENTO DE OBJETIVOS

| Objetivo específico | Producto | Observaciones |
|---|---|---|
| Identificar problemas, necesidades y oportunidades de la Universidad Tecnológica de Pereira, con relación a la federación de identidad. | Identificación de problemas y necesidades de mayor relevancia que tiene la UTP respecto a los recursos computacionales. Expuesto en el capítulo 5: sección 5.1.1 | Se realizó en entrevista guiada con el vicerrector administrativo y financiaro, la jefe de gestión de tecnologías informáticas y sistemas de información, y el director del centro de recursos informáticos y educativos. |
| | Identificación de oportunidades expuesto en el capítulo 5: sección 5.1.2.9 | Se tomó como base las fichas con capacidades de los grupos de investigación que fueron obtenidas por la vicerrectoría de investigaciones y extensión. |
| Seleccionar tecnologías existentes para federación de identidad que satisfagan los problemas, necesidades | Selección del estándar a utilizar. Expuesto en el capítulo 5: Sección 5.2.5 | Se realizó caracterización de las tecnologías mas utilizadas enfederación de identidad. Se realizó un cuadro comparativo y a |

| Objetivo específico | Producto | Observaciones |
|---|---|---|
| u oportunidades del objetivo anterior. | | través de mecanismo formal para toma de deciciones se seleccionó SAML. |
| Construir un esquema arquitectónico para la implementación de federación de identidad en la UTP. | Definición de una arquitectura para la federación de identidad. Expuesto en el capítulo 5: Secciones 5.3.2 y 5.3.3 | Se expresó la arquitectura con un modelo BPMN. |
| Implementar un prototipo funcional de federación de identidad para el esquema arquitectónico definido | Diseño del prototipo funcional. Expuesto en el capítulo 5: Secciones 5.4.1 y 5.4.5 | Se realizó implentación del prototipo, alcanzando la publicación del IdP de UTP hacía eduGAIN. La publicación del servicio se realizó sólo local debido a las eduGAIN sólo permite publicar servicios a través de COLFIRE, y actualmente no cuentan con el servicio de |

| Objetivo específico | Producto | Observaciones |
|---|---|---|
| | | descubrimiento de servicios implementado. |

***Tabla 23*** *Cumplimiento de Objetivos*

# 7 CONCLUSIONES

Mediante la valoración realizada al grupo objetivo utilizando estrategias como la entrevista, socialización y el análisis documental fue posible identificar problemas, necesidades y oportunidades. En ese sentido y como primera instancia, se identificaron aspectos relacionados a los problemas y necesidades destacándose la ejecución presupuestal atomizada, el aislamiento de los recursos computacionales costosos existentes en los grupos de investigación, además del desaprovechamiento de recursos y servicios. Por lo anterior, este trabajo presenta un escenario de difusión y colaboración de los recursos y servicios computacionales existentes en la UTP, de este modo se permite reorientar el enfoque presupuestal de los grupos de investigación, con una apuesta más comunitaria, evitando por ejemplo la compra repetida de recursos y servicios existentes. Como segunda instancia y con relación a las oportunidades se identificaron 137 recursos computacionales con posibilidades de ser federados en el escenario de difusión propuesto en este trabajo.

A través de la revisión de la literatura acerca de las tecnologías relacionadas con la federación de identidad, fue posible decantar los estándares OAUTH2, OIDC y SAML. De los anteriores se seleccionó el estándar SAML como el marco tecnológico adecuado para la implementación de federación de identidad en la UTP. Se destaca fuertemente el uso del estándar SAML en la red interfederada eduGAIN y la red académica RENATA en Colombia.

Como elemento central de este trabajo se ha construido un esquema arquitectónico para la implementación de la federación de identidad en la Universidad Tecnológica de

Pereira. La arquitectura propuesta está basada tecnológicamente en el estándar SAML y está expresado a través de tres escenarios de implementación. El primer escenario es para una entidad que sólo consume servicios. El segundo escenario es para una organización que sólo pública servicios, no los consume. El último es un escenario completo donde la institución consume y publica servicios. Estos escenarios facilitan que una institución pueda adaptar la solución de acuerdo con su nivel de madurez tecnológica.

De acuerdo con la arquitectura propuesta, se ha elaborado y desplegado un prototipo funcional de federación de identidad que servirá como base para su implementación en la Universidad Tecnológica de Pereira. En especial, será de gran utilidad para federar recursos y servicios identificados en los grupos de investigación y para facilitar a la Administración optimizar los recursos de inversión. Adicional, se ha incluido una puesta en producción del escenario 1 de la arquitectura propuesta donde la organización puede consumir servicios de las instituciones que pertenezcan a la red académica de federación de identidad eduGAIN. Con el propósito de presentar el funcionamiento del escenario 2, se ha desplegado un prototipo para federar servicios, con lo que se logrará aprovechar las capacidades identificadas en los grupos de investigación. Ahora bien, de acuerdo con la madurez tecnológica de una organización, se pueden unir estos dos escenarios para tener una solución que permita tanto consumir como federar servicios.

Finalmente, como aporte a la comunidad de desarrollo de software, es importante resaltar que para facilitar la federación de identidad, se debe incluir el estándar SAML en las aplicaciones para aprovechar la arquitectura propuesta.

# 8 APORTE Y TRABAJO FUTURO

**Aporte:**

- La arquitectura propuesta para la federación de identidad propone escenarios/estados que facilitan la implementación en la institución de acuerdo con su grado de madurez en esta tecnología. Esta arquitectura se propone como una vista macro en donde su aplicación encaja con la red interfederada eduGAIN a través de la federación COLFIRE de Colombia.

- El piloto se ha llevado a la puesta en producción con el componente de proveedor de identidad a través de la federación COLFIRE y hacia eduGAIN. Esto permite que la comunidad académica de la UTP pueda acceder a los servicios federados por medio de eduGAIN por cualquiera de sus instituciones asociadas.

**Trabajo futuro:**

- Trabajar en conjunto con el personal técnico de RENATA para implementar el servidor de descubrimiento de Colombia y ponerlo al servicio de las instituciones académicas que deseen federar sus servicios.

- A partir de las capacidades identificadas en los grupos de investigación, realizar una revisión más detallada que permita identificar los servicios que tengan viabilidad técnica, administrativa y legal, para que sean federados.

- Proyección de difusión académica

    - Sometimiento de artículo derivado del trabajo de investigación en revista indexada.
    - Sometimiento del trabajo en el Congreso Colombiano de Computación a realizar en 2020.
    - Solicitar espacio para workshop en el Congreso Colombiano de Computación a realizar en 2020, presentando el prototipo desplegado en Docker.

# 9 REFERENCIAS BIBLIOGRÁFICAS


Anicas, M. (2020). Una introducción a OAuth 2 | DigitalOcean. Retrieved February 2, 2020, from https://www.digitalocean.com/community/tutorials/una-introduccion-a-oauth-2-es

Barker, M., Olabarriaga, S. D., Wilkins-Diehr, N., Gesing, S., Katz, D. S., Shahand, S., … Costa, A. (2019). The global impact of science gateways, virtual research environments and virtual laboratories. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.12.026

Chun, K. L., & Katuk, N. (2014). A Usability Study of Social Media Credentials As A Single-Sign-On Mechanism: Student Access to Online Teaching Materials. *Journal of Industrial and Intelligent Information*, *2*(3), 217–221. https://doi.org/10.12720/jiii.2.3.217-221

Colfire - Red RENATA. (2020). Retrieved February 7, 2020, from https://www.renata.edu.co/colfire/

Daryanani, A., & Lopez, D. R. (2008). Cross-federated Access to Campus Services with eduGAIN. *IBERGRID: 2ND IBERIAN GRID INFRASTRUCTURE CONFERENCE PROCEEDINGS*.

Database and Application Security XV. (2002). In *Database and Application Security XV*. https://doi.org/10.1007/978-0-387-35587-0

De Angelis, F., Falcioni, D., Ippoliti, F., Marcantoni, F., & Re, B. (2013). Federated Digital Identity in Smart University: The Unicam Experience. *7th International Conference on Methodologies, Technologies and Tools Enabling e-Government (MeTTeG 2013)*.

eduGAIN – enabling worldwide access. (2020). Retrieved February 6, 2020, from https://edugain.org/

Familiar, B. (2015). *Microservices, IoT, and Azure Leveraging DevOps and Microservice Architecture to Deliver SaaS Solutions*. Retrieved from www.apress.com/bulk-sales.

Foundation, O. (2020). OpenID Connect | OpenID. Retrieved February 4, 2020, from https://openid.net/connect/

IETF. (2012). RFC 6749 - The OAuth 2.0 Authorization Framework. Retrieved February 4, 2020, from https://tools.ietf.org/html/rfc6749

miniOrange Secure It Right : Identity and Access Management Solution. (2020). Retrieved February 8, 2020, from https://www.miniorange.com/

OASIS. (2020). FrontPage - SAML Wiki. Retrieved February 4, 2020, from https://wiki.oasis-open.org/security/FrontPage

OpenLDAP. (2020). OpenLDAP, Main Page. Retrieved February 5, 2020, from https://www.openldap.org/

Pérez Méndez, A., Marín López, R., & López Millán, G. (2016). Providing efficient SSO to cloud service access in AAA-based identity federations. *Future Generation Computer Systems*, *58*, 13–28. https://doi.org/10.1016/j.future.2015.12.002

SEI Administrative Agent. (2010). *CMMI ® para Desarrollo, Versión 1.3 Equipo del Producto CMMI*. Retrieved from http://www.sei.cmu.edu

Sermersheim, J. (2006). Lightweight Directory Access Protocol (LDAP): The Protocol.

*The Internet Engineering Task Force*.
Shaer, C. (1995). Single sign-on. *Network Security*, *1995*(8), 11–15. https://doi.org/10.1016/1353-4858(96)89743-1
UY, A. de G. E. y S. de la I. y el C.-. (2020). Integración con servicio de autenticación - Wiki - Seguridad. Retrieved February 2, 2020, from https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Integración+con+servicio+de+autenticación/pop_up
Vicerrectoría de investigaciones, I. y extensión. (2020). Vicerrectoría de Investigaciones, Innovación y Extensión :: Grupos. Retrieved February 2, 2020, from https://www.utp.edu.co/vicerrectoria/investigaciones/investigaciones/grupos.html
Wierenga, K., & Florio, L. (2005). Eduroam: Past, present and future. *TERENA Networking Conference 2005: The World of Pervasive Networking, TNC 2005*.
Wilson, Y., & Hingnikar, A. (2019). Solving Identity Management in Modern Applications. In *Solving Identity Management in Modern Applications*. https://doi.org/10.1007/978-1-4842-5095-2
Wilson, Y., Hingnikar, A., Wilson, Y., & Hingnikar, A. (2019). The Hydra of Modern Identity. In *Solving Identity Management in Modern Applications*. https://doi.org/10.1007/978-1-4842-5095-2_1

# 10 ANEXOS

Se han publicado los archivos de configuración y las guías de implentación en el repositorio GITHUB. A continuación, el enlace:

https://github.com/jhonnier-sys/federation